CA Process Automation

Guia de Administrador de Conteúdo

Release 04.2.00

technologies

Referências a produtos da CA Technologies

Este documento faz referência aos seguintes produtos da CA Technologies:

- CA Catalyst para o CA Service Desk Manager (CA Catalyst Conector do CA SDM)
- CA Client Automation (anteriormente CA IT Client Manager)
- CA Configuration Automation (anteriormente, CA Cohesion® Application Configuration Manager)
- CA CMDB
- CA eHealth®
- CA EEM (Embedded Entitlements Manager)
- CA Infrastructure Insight (anteriormente Bundle: CA Spectrum IM & CA NetQoS Reporter Analyzer combinados)
- CA NSM
- CA Process Automation (anteriormente, CA IT Process Automation Manager)
- CA Service Catalog
- CA SDM (CA Service Desk Manager)
- CA Service Operations Insight (CA SOI) (anteriormente CA Spectrum® Service Assurance)
- CA SiteMinder®
- CA Workload Automation AE

Entrar em contato com o Suporte técnico

Para assistência técnica online e uma lista completa dos locais, principais horários de atendimento e números de telefone, entre em contato com o Suporte técnico pelo endereço http://www.ca.com/worldwide.

Alterações na documentação

Foram feitas as seguintes atualizações de documentação desde a última release desta documentação:

- Introdução de novos usuários ao CA Process Automation (na página 60) - Este tópico existente foi atualizado para incluir referências à nova *Referência de interface do usuário*, que contém descrições dos campos.
- Exemplo: Um indivíduo em dois Active Directories referenciados (na página 65) - Este novo tópico fornece um exemplo de usuários do CA Process Automation que estão sendo referenciados pelo CA EEM a partir de vários Microsoft Active Directories, nos quais o mesmo usuário está definido para mais de um AD referenciado.
- Configurar as definições de segurança do CA EEM para o domínio (na página 140) - Este tópico existente foi atualizado para incluir o valor de domínio padrão do Active Directory, um campo que é válido somente quando se o CA EEM estiver configurado para usar vários domínios do Microsoft Active Directory.
- Configurar propriedades do domínio (na página 146) - Este tópico existente foi atualizado para incluir novos campos que estão relacionados à configuração do grupo de hosts e à limpeza de dados de relatórios. Outros tópicos atualizados de forma semelhante para a configuração do grupo de hosts:
  - Configurar propriedades do ambiente (na página 157)
  - Configurar as propriedades do touchpoint do orquestrador (na página 174)
  - Configurar propriedades do host do orquestrador (na página 181)
  - Garantir o processamento eficiente de referências de grupo de hosts (na página 260)
- Instalar um agente de forma interativa (na página 202) - Este tópico existente foi atualizado para documentar uma nova caixa de seleção para especificar se o agente deverá usar a comunicação simplificada (com NGINX ou F5) ou a comunicação obsoleta (com o Apache ou F5). Também é observado que o Windows oferece suporte ao jre7, bem como ao jre6. Outros tópicos atualizados para abordar novas comunicações:
  - Configurar propriedades do agente (na página 207)
  - Sobre a comunicação do agente (na página 217)
  - Configurar os agentes para usarem a comunicação simplificada (na página 217)
  - Configurar os agentes para usarem a comunicação obsoleta (na página 218)
- Cenário: Configurar touchpoints para criação e produção (na página 221) - Este novo cenário combina as informações existentes para mostrar como as opções de configuração usadas em um ambiente de produção são diferentes das usadas em um ambiente de criação.

- Quando evitar usar as referências do grupo de hosts como destinos (na página 262) - Este novo tópico aborda o impacto de especificar um endereço IP como destino de um operador para que um processo seja distribuído para um ambiente ou domínio em que o destino seja um host diferente. Os processos exportados e importados como um pacote de conteúdo não podem ser modificados.
- Configurando categorias do operador (na página 270) - Todos os tópicos nesta seção existente foram refatorados para remover as descrições dos campos que foram adicionados à *Referência de interface de usuário*.
- Planejar a estrutura de pastas (na página 346) - Este tópico existente foi reescrito para acomodar os requisitos de exportação de uma pasta como um pacote de conteúdo. Esse novo método de exportação requer que todos os objetos de uma versão da release estejam na mesma pasta.
- Como preparar o ambiente de produção para uma nova release (na página 358) - Esse processo existente foi reescrito para a nova opção, exportar a pasta como um pacote de conteúdo, que substituiu exportar um objeto de automação do pacote. Os tópicos relacionados incluem:
  - Sobre a exportação e a importação de um pacote de conteúdo (na página 359)
  - Cenário: exportar e importar objetos em um pacote de conteúdo (na página 360) (Este cenário inclui um exemplo, bem como os conceitos e procedimentos relacionados.)
- Limpar objetos e pastas (na página 376) - Este tópico existente foi atualizado para incluir o que acontece quando você tenta limpar objetos reservados. Esta ação é recém-suportada no CA Process Automation r4.2.

Índice

Capítulo 1: Introdução 15

Capítulo 2: Visão geral para administradores 23

Capítulo 3: Administrar a segurança básica do CA EEM 43

Capítulo 5: Administrar o domínio do CA Process Automation. 137

Capítulo 6: Administrar os ambientes 155

Capítulo 7: Administrar Orquestradores 169

Capítulo 8: Administrar agentes 197

Capítulo 9: Administrar touchpoints 219

Capítulo 13: Administrar disparadores 313

Capítulo 14: Gerenciar recursos de usuário 327

Capítulo 15: Auditorar ações do usuário 335

Capítulo 16: Administrar objetos da biblioteca 345

Capítulo 1: Introdução

Quando você inicialmente instala o CA Process Automation com o CA EEM configurado com um armazenamento de usuários interno, há um usuário administrador padrão com as seguintes credenciais:

Nome de usuário

pamadmin

Senha

pamadmin

Você pode navegar para uma instância de produto recém-instalada e efetuar logon com essas credenciais. Uma abordagem mais adequada é criar uma conta de usuário no CA EEM durante sua primeira sessão e, em seguida, efetuar logon no CA Process Automation com as credenciais definidas.

Após efetuar logon, defina as configurações para administrar a segurança e configurar o domínio.

Esta seção contém os seguintes tópicos:

Efetuar logon no CA EEM como o usuário EiamAdmin

O usuário EiamAdmin pode efetuar logon no CA EEM, bem como gerenciar identidades (contas de usuário) e diretivas de acesso.

Siga estas etapas:

1. Vá até o URL da instância do CA EEM que o CA Process Automation utiliza:

   `https://nome_do_host:5250/spin/eiam`

   nome do host

   Define o nome do host ou o endereço IP do servidor onde o CA EEM está instalado.

   Observação: para determinar o nome do host do CA EEM usado pelo CA Process Automation, consulte o campo Servidor de back-end do CA EEM, na guia Configuração e na subguia Segurança do CA Process Automation.

2. Na lista suspensa Aplicativo, selecione o valor que você configurou para o Nome do aplicativo do EEM durante a instalação.

   Observação: esse é o nome que você usou para registrar o CA Process Automation com o CA EEM.

3. Digite **EiamAdmin** e a senha que você definiu para o usuário EiamAdmin.
4. Clique em Efetuar logon.

Criar a primeira conta de administrador

É possível criar sua própria conta de usuário do CA Process Automation no CA EEM e autorizar o acesso completo (Administrador) ao CA Process Automation.

Siga estas etapas:

1. Efetue logon no CA EEM como o usuário EiamAdmin (na página 16).
2. Clique na guia Gerenciar identidades.
3. Clique no ícone ao lado de Usuários na paleta Usuários.

   A página Novo usuário é aberta.

4. Digite a ID de usuário no campo Nome que deseja inserir como o Nome de usuário quando você efetua logon no CA Process Automation.
5. Clique em Adicionar detalhes do usuário do aplicativo.

6. Selecione PAMAdmins em Grupos de usuários disponíveis e clique em > para movê-lo para Grupos de usuários selecionados.

   O grupo concede acesso completo a todos os recursos do CA Process Automation.

7. Digite seus próprios detalhes na seção Detalhes do usuário global do perfil da conta de usuário.

8. (Opcional) Preencha o campo Associação a grupo global se usar o CA Process Automation com outro produto da CA Technologies que usa este CA EEM.

9. Crie a senha na área de autenticação que deseja inserir quando você efetua logon no CA Process Automation.

10. (Opcional) Preencha os campos restantes na página Novo usuário.

11. Clique em Salvar.

    Uma mensagem de confirmação indica "Detalhes do usuário global criados com êxito". Detalhes do usuário global criados com êxito.

12. Clique em Fechar.

13. Clique em Logoff.

Vá até o CA Process Automation e efetue logon.

O URL usado para acessar o CA Process Automation depende se o orquestrador de domínio está configurado com um nó (não agrupado) ou vários nós (agrupado). É possível navegar diretamente para um CA Process Automation não agrupado. Para um CA Process Automation agrupado, procure o balanceador de carga associado. É possível acessar todos os orquestradores no domínio iniciando o URL para o orquestrador de domínio ou para o balanceador de carga para o orquestrador de domínio.

Siga estas etapas:

1. Procure o CA Process Automation.

   - Para uma comunicação segura, use a sintaxe a seguir:
     `https://`*`server`*`:`*`port`*`/itpam`

     Exemplos:
     ```
     https://Orchestrator_host:8443/itpam
     https://loadBalancer_host:443/itpam
     ```

   - Para uma comunicação básica, use a sintaxe a seguir:
     `http://`*`server`*`:`*`port`*`/itpam`

     Exemplos:
     ```
     http://Orchestrator_host:8080/itpam
     http://loadBalancer_host:80/itpam
     ```

   A página de logon do CA Process Automation é exibida.

2. Digite as credenciais de sua conta de usuário.

   Observação: se o CA EEM estiver configurado para fazer referência a usuários de vários Microsoft Active Directories e o CA Process Automation não aceitar seu nome de usuário não qualificado, digite o nome de sua entidade principal, que é *nome_do_domínio**nome_do_usuário*.

3. Clique em Efetuar logon.

   O CA Process Automation é exibido. A guia Início é exibida.

Definir idioma e formatos de data e hora

Por padrão, os dados de data e hora para o orquestrador de domínio são exibidos no fuso horário do navegador. Durante a sua primeira sessão de logon, você pode definir suas preferências para os formatos de data e hora e para idioma.

Observação: o produto armazena todas as datas e horas em UTC (Coordinated Universal Time - Horário Universal Coordenado).

Siga estas etapas:

1. Vá até o CA Process Automation e efetue logon (na página 18), se ainda não estiver conectado.
2. Na barra de ferramentas, clique em seu nome de usuário.
3. Na caixa de diálogo Configurações do usuário, selecione suas preferências para os formatos de data e hora.
4. Verifique e altere a configuração de idioma, se necessário.
5. Clique em Salvar e fechar.
6. Clique em OK.
7. Clique em Logoff.

   Suas configurações serão aplicadas quando você fizer logon novamente.

Atualizar conteúdo pronto para uso

O novo conteúdo predefinido (pronto para uso) fica disponível periodicamente. Apenas um administrador pode importar um novo conteúdo predefinido. Para garantir que a pasta PAM_PreDefinedContent contém o conteúdo predefinido mais recente, repita o procedimento de atualização ocasionalmente.

Siga estas etapas:

1. Excluir conteúdo previamente importado.
   a. Clique na guia Biblioteca.
   b. Selecione a pasta PAM_PreDefinedContent, clique em Excluir e, em seguida, clique em Sim na mensagem de confirmação.

      A pasta PAM_PreDefinedContent será movida para a lixeira. (Recolha a árvore de pastas para ver a lixeira.)
   c. Selecione a pasta PAM_PreDefinedContent na Lixeira e clique em Limpar.
2. Clique na guia Início.

3. Clique em Explorar o conteúdo pronto para uso.
4. Clique em Sim para confirmar a importação.

   O processo de importação cria a pasta PAM_PreDefinedContent com o conteúdo mais recente no diretório raiz da guia Biblioteca.

Controlar o intervalo de tempo limite

Você pode alterar o intervalo de tempo limite do produto. Por padrão, o produto efetua logoff automaticamente após 15 minutos de inatividade.

Siga estas etapas:

1. Efetue logon como administrador no servidor em que o orquestrador de domínio está instalado.
2. Vá até a seguinte pasta:

   install_dir/server/c2o/.config

   install_dir

   Define o caminho em que o orquestrador de domínio está instalado.

3. Abra o arquivo OasisConfig.properties com um editor.
4. Use Localizar para encontrar a seguinte propriedade:

   managementconsole.timeout

5. Altere o valor da propriedade.
6. Salve o arquivo e saia.
7. Reinicie o serviço do orquestrador:
   a. Interrompa o orquestrador (na página 193).
   b. Inicie o orquestrador (na página 194).

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Configurações recomendadas do navegador IE para autenticação de passagem NTLM

As configurações recomendadas do navegador Windows Internet Explorer (IE) para autenticação de passagem NTLM se aplicam aos seguintes casos, em que o CA EEM aponta para um Active Directory externo:

- O CA EEM usa autenticação de passagem NTLM para autenticar usuários globais do CA Process Automation.
- Os usuários usam o Internet Explorer para navegar para o CA Process Automation.
- O IE solicita um nome de usuário e uma senha.

Siga estas etapas:

1. No menu Ferramentas do IE, selecione Opções da internet e clique na guia Segurança.
2. Selecione o ícone Intranet local e, em seguida, clique em Nível personalizado.

   A caixa de diálogo Configurações de segurança - Zona da intranet local é exibida.
3. Role para Autenticação do usuário e selecione Logon automático somente na zona da intranet.
4. Adicione o URL do CA Process Automation à zona da intranet local.

Sobre este guia

O *Guia de Administrador de Conteúdo* se concentra nas tarefas executadas pelos usuários com as funções a seguir:

- Administradores do CA EEM que configuram o CA EEM para o CA Process Automation.
- Administradores de conteúdo do CA Process Automation com direitos de administrador de domínio, administrador de configuração do ambiente e administrador de conteúdo do ambiente.

As tarefas do administrador de conteúdo incluem:

- Configuração de segurança.
- Configurando o produto para oferecer suporte ao desenvolvimento de conteúdo e uso de produção.

Antes de começar a usar este guia, certifique-se de que as tarefas de instalação e configuração descritas no *Guia de Instalação* do CA Process Automation foram executadas.

Observações:

- Para os fluxos de trabalho relacionados à configuração de um novo ambiente de criação de conteúdo ou um novo ambiente de produção, consulte a *Ajuda online*.
- Para obter informações sobre como os criadores de conteúdo usam os métodos de serviços web, consulte a *Referência da API de serviços web*.
- Para obter informações sobre como os criadores de conteúdo criam processos e outros objetos de automação, consulte o *Guia do Criador de Conteúdo*.
- Para obter informações sobre operadores, consulte a *Referência do Criador de Conteúdo*.
- Para obter informações sobre como os usuários de produção usam o produto em um ambiente de produção, consulte o *Guia do Usuário de Produção*.
- Para obter informações sobre como os criadores usam a guia Operações durante a criação de conteúdo, consulte o *Guia do Usuário de Produção*.

Capítulo 2: Visão geral para administradores

Esta seção contém os seguintes tópicos:

Visão geral das tarefas de administração

O CA Process Automation fornece a interface principal para desenvolvimento de conteúdo. Os administradores do sistema e administradores de conteúdo usam o CA Process Automation para as seguintes atividades:

- Administrar a segurança.

  A segurança para o CA Process Automation envolve a autenticação de usuário ao fazer logon e acesso com base em funções. Você define contas de usuário, grupos personalizados e diretivas que concedam permissões por meio do CA EEM.

- Administrar o domínio.

  Domínio é o termo usado para descrever a visão empresarial de todo o sistema do CA Process Automation, incluindo orquestradores, agentes e bibliotecas de processos. A administração do domínio inclui a adição de ambientes, a remoção de agentes e touchpoints em massa não utilizados e o gerenciamento das propriedades do domínio.

- Configurar os Orquestradores.

  Um *orquestrador* é o componente do mecanismo do CA Process Automation que faz a leitura da biblioteca de processos e executa os processos. O primeiro orquestrador do CA Process Automation que você instala é o orquestrador de domínio. É possível adicionar mais nós para o orquestrador de domínio para adicionar potência de processamento e balanceamento de carga. Se os usuários estiverem geograficamente dispersos, considere adicionar um novo orquestrador padrão em cada local.

- Criar e configurar ambientes.

  Um *ambiente* é uma partição opcional do domínio que separa o desenvolvimento de conteúdo. Ambientes podem ser criados para desenvolvimento, teste e produção ou para diferentes unidades de negócios. A configuração inclui adicionar touchpoints e criar grupos de touchpoints.

- Configurar os agentes.

  Um *agente* é o software do CA Process Automation instalado em um host de rede. Os orquestradores que executam processos podem executar determinadas etapas do processo em hosts do agente ou em hosts remotos, com os quais os agentes têm conexões SSH. Uma configuração inclui a associação de touchpoints, touchpoints do proxy ou grupos de hosts aos agentes.

- Mapear e configurar touchpoints.

  Um *touchpoint* é uma entidade lógica usada em definições de operador para representar o agente de destino ou o orquestrador no qual alguma parte do processo é executada. É possível mapear um touchpoint para muitos agentes de uma única vez e diferentes agentes ao longo do tempo. Os touchpoints fornecem flexibilidade na implementação de processos e, ao mesmo tempo, reduzem os requisitos de manutenção para os processos.

- Mapear e configurar os touchpoints do proxy e grupos de hosts.

  Hosts remotos, ou seja, hosts sem um agente instalado, podem ser direcionados para executar operações como parte de um processo em execução. Para ativar a conectividade, estabeleça o acesso ao SSH de um host com um agente para o host remoto. No host com o agente, configure um touchpoint do proxy ou um grupo de hosts. Um operador pode usar como destino um host com seu nome de touchpoint do proxy. Um grupo de hosts faz referência a hosts remotos. Um operador pode usar como destino um host remoto com seu FQDN ou um endereço IP.

  Observação: consulte Sintaxe de nomes de host DNS (na página 393).

- Procurar na biblioteca.

  Uma *biblioteca* é o repositório que contém os objetos de operadores e scripts que os criadores de conteúdo usam para criar processos. Processos e outros objetos de automação são armazenados na biblioteca.

- Administrar objetos de automação em bibliotecas.

  Objetos de automação definem o processamento, a programação, o monitoramento, o registro e outros elementos configuráveis de um pacote do CA Process Automation. Os objetos de automação são armazenados na biblioteca de um orquestrador específico, em uma arquitetura não agrupada. A administração de objetos de automação inclui a definição opcional das configurações de segurança em uma pasta ou objeto da biblioteca a fim de controlar o acesso a grupos e usuários designados.

- Gerenciar a segurança para objetos de automação.

  É possível criar diretivas personalizadas do CA EEM para objetos de automação. Por exemplo, ativar a segurança do touchpoint e criar diretivas de segurança do touchpoint no CA EEM para limitar quem pode executar determinados operadores em destinos especificados com valores altos. Ativar a segurança de tempo de execução e usar Definir proprietário para conceder os direitos de iniciar o processo apenas ao proprietário do processo.

- Administrar processos.

  Um exemplo de administração de processos é anular processos com falha na exibição de processos.

Visão geral das guias

A disponibilidade de guias específicas na interface do usuário do produto depende dos direitos de acesso concedidos ao usuário conectado. Quando você efetua logon no produto pela primeira vez, a interface do usuário exibe as guias que este tópico descreve.

Observação: a maioria das tarefas de configuração e administração é executada na guia Configuração. Para conhecer os fluxos de tarefas relacionados a cada guia, consulte a *Ajuda online*.

Página inicial

A guia Início ajuda a acessar rapidamente os objetos com os quais você está trabalhando. Você pode usar outros links para obter acesso rápido a informações de interesse geral.

Biblioteca

Normalmente, os administradores de conteúdo criam pastas e concedem direitos de acesso a elas.

Observação: os criadores de conteúdo criam objetos e acessam esses objetos para edição nas pastas da guia Biblioteca. A guia Criador é o editor para objetos de processo.

Pastas

Um administrador normalmente configura uma estrutura de pastas no ambiente de criação. As pastas contêm subpastas e objetos de automação. A prática recomendada é criar uma pasta para cada processo que você automatiza, com uma subpasta para cada versão da release desse processo. As pastas em nível de processo podem estar no nível raiz.

A pasta que contém a versão da release de um processo é exportada como pacote de conteúdo e, em seguida, importada para o ambiente de produção. O processo de importação duplica a estrutura de pastas no ambiente de produção. A diferença é que a biblioteca de produção contém apenas a versão da release do processo e objetos relacionados. Pastas não são criadas manualmente na biblioteca de produção.

Lixeira

A Lixeira na parte inferior do nó Orquestrador contém pastas e objetos que foram excluídos. Quando você clica em Lixeira, pode selecionar as pastas e os objetos excluídos para eliminar (remover permanentemente) da biblioteca ou para restaurar à biblioteca.

Pesquisar

Defina pasta, palavra-chave ou critérios de data com os quais pesquisar objetos de conteúdo no campo Pesquisar.

Índice

Os criadores de conteúdo criam instâncias dos objetos de automação selecionados em uma pasta. Eles abrem as instâncias criadas na parte de conteúdo da guia Biblioteca.

Designer

Os criadores de conteúdo criam um processo planejado na guia Criador.

Operações

A guia Operações é usada pelos usuários no grupo Usuários de produção. inclui as seguintes paletas:

Links

Exibe as informações no painel direito para os seguintes links padrão:

Instâncias de processo

Instâncias de processos que foram iniciados. O gráfico de barras no painel Instâncias de processo exibe os operadores por estado. O painel Instâncias de processo também exibe os detalhes de cada operador.

Operadores

Operadores em processos iniciados e tarefas de programações. O gráfico de barras no painel Operadores exibe os operadores por estado. O painel Operadores também exibe os detalhes de cada operador.

Tarefas

As tarefas que são atribuídas a usuários e grupos. Todos os usuários podem visualizar sua lista de tarefas específica, as listas de tarefas de grupos aos quais eles pertencem e as tarefas atribuídas a outros usuários. Os administradores atribuem tarefas a usuários ou grupos. Um usuário obtém uma tarefa atribuída e responde à notificação de interação do usuário.

Programações ativas

Programações que iniciaram os processos ativos.

Programações globais

Programações que podem ser usadas por qualquer usuário para iniciar qualquer processo ou operadores selecionados. É possível filtrar a exibição por data, orquestrador ou touchpoint do agente, bem como por programação atual ou arquivada.

Solicitações iniciais

Solicita que processos especificados sejam iniciados sob demanda.

Pacotes de conteúdo

Todos os usuários podem monitorar objetos que são importados para o ambiente como pacotes de conteúdo. Quando você clica em um pacote de conteúdo no painel esquerdo, as propriedades do pacote são exibidas no painel direito.

Observação: você pode exibir informações da versão da release dos seguintes itens incluídos nos pacotes de conteúdo:

- Instâncias do processo
- Programações ativas
- Programações globais
- Solicitações iniciais

O produto exibe o nome do pacote de conteúdo e a versão da release do pacote de conteúdo para cada objeto.

Exibição de processos

Todos os usuários podem monitorar processos em todos os estados, programações ativas, operadores, solicitações iniciais, conjuntos de dados, recursos e operadores personalizados.

Solicitações iniciais

Os usuários podem visualizar um gráfico de barras de instâncias de solicitação inicial em fila, em execução, concluídas e com falha. Em uma barra selecionada, os usuários podem visualizar o nome da instância, a hora programada, o estado, a hora de início e de término e o nome do usuário.

Conjunto de dados

Os usuários podem exibir a estrutura de um conjunto de dados selecionado e seus pares de nome/valor.

Recursos

Os usuários podem selecionar um objeto de recursos e, em seguida, usar o painel direito para substituir os valores exibidos em Quantidade e Usado manualmente. Os usuários também podem alterar o Estado.

Programações

Os usuários podem selecionar uma programação e, em seguida, usar o painel direito para definir as seguintes propriedades:

- A data de execução.
- Se deseja mostrar a atividade para todos os nós ou para um orquestrador selecionado.
- Se deseja exibir as programações arquivadas.

Configuração

O administrador é responsável por configurar o acesso ao CA Process Automation na guia Configuração. Por padrão, os ambientes, orquestradores e agentes herdam as configurações definidas pelos administradores no nível do domínio. Os operadores herdam as configurações definidas pelos administradores no nível de categoria do operador. A guia Configuração contém as seguintes paletas:

Navegador de configuração

Exibe os seguintes nós:

Domain

Configure o domínio, o ambiente padrão, o touchpoint do orquestrador, os touchpoints do agente e do proxy, e os grupos de hosts.

Orquestradores

Configure o orquestrador de domínio e os outros orquestradores instalados.

Agentes

Configure associações e configurações de todos os agentes instalados.

Gerenciar recursos de usuário

O administrador do sistema deverá acessar a pasta Recursos do usuário para adicionar ou atualizar os scripts usados no desenvolvimento de conteúdo. Os administradores podem carregar arquivos JAR para a pasta Recursos do agente ou Recursos do orquestrador. O produto compartilha os arquivos carregados quando você reinicia os agentes ou orquestradores.

Instalações

O administrador do sistema instala outros orquestradores ou nós de agrupamento para o orquestrador de domínio ou outros orquestradores. Os administradores também instalam agentes.

Relatórios

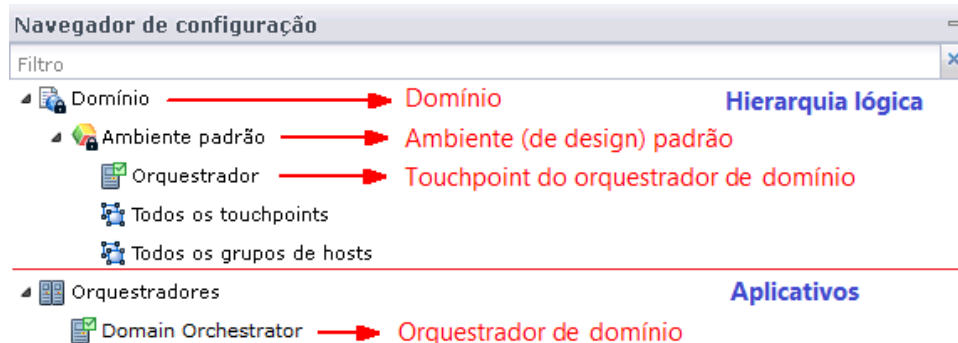
Todos os usuários podem acessar os relatórios predefinidos ou fazer upload de relatórios personalizados desenvolvidos com o BIRT RCP Designer.

Relacionamentos entre os componentes

Como um administrador do CA Process Automation, suas responsabilidades incluem:

- Configuração: domínio, ambiente padrão, ou orquestrador.
- Instalação e configuração para criar o domínio: outros orquestradores e agentes.
- Criação e configuração de entidades lógicas: ambientes, touchpoints (incluindo touchpoints do proxy) e grupos de hosts.

Antes de começar, é útil entender os relacionamentos entre essas entidades físicas e lógicas. A paleta Navegador de configuração na guia Configuração exibe uma árvore da hierarquia lógica, o nó Orquestradores e o nó vazio Agentes. A hierarquia lógica consiste inicialmente sob o nó Domínio com o nó Ambiente padrão. O nó Ambiente padrão expandido exibe o orquestrador, o nó vazio Todos os touchpoints vazios em branco e o nó vazio Todos os grupos de hosts.

Navegador de configuração
Filtro
Domínio → Domínio — Hierarquia lógica
Ambiente padrão → Ambiente (de design) padrão
Orquestrador → Touchpoint do orquestrador de domínio
Todos os touchpoints
Todos os grupos de hosts
Orquestradores — Aplicativos
Domain Orchestrator → Orquestrador de domínio

O domínio é o nó raiz da hierarquia lógica. Todos os orquestradores que você instala são exibidos sob o nó Orquestradores. Todos os agentes que você instala são exibidos sob o nó Agentes (não exibido).

O termo touchpoint refere-se à associação entre um orquestrador e um ambiente; um touchpoint também se refere à associação entre um agente e um ambiente. A ilustração mostra o Navegador de configuração exibido logo após a primeira instalação do CA Process Automation. Portanto, não inclui agentes ou touchpoints do agente. Os criadores de conteúdo usam os touchpoints como destinos nos processos que automatizam. (O uso e as vantagens dos touchpoints são informados em outro lugar.)

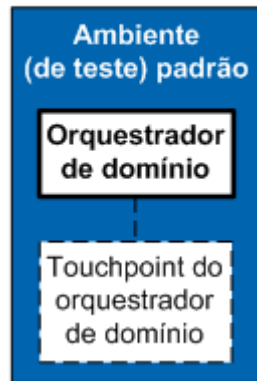
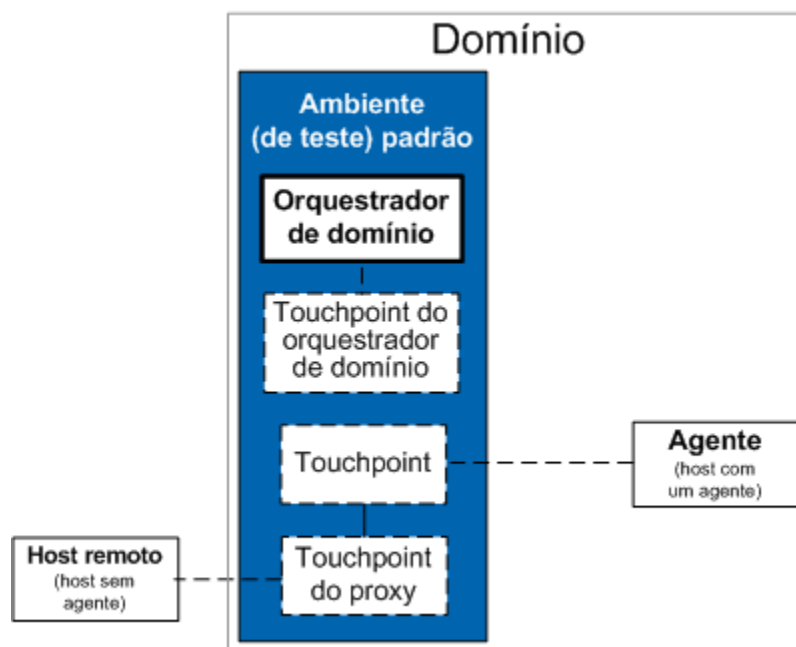
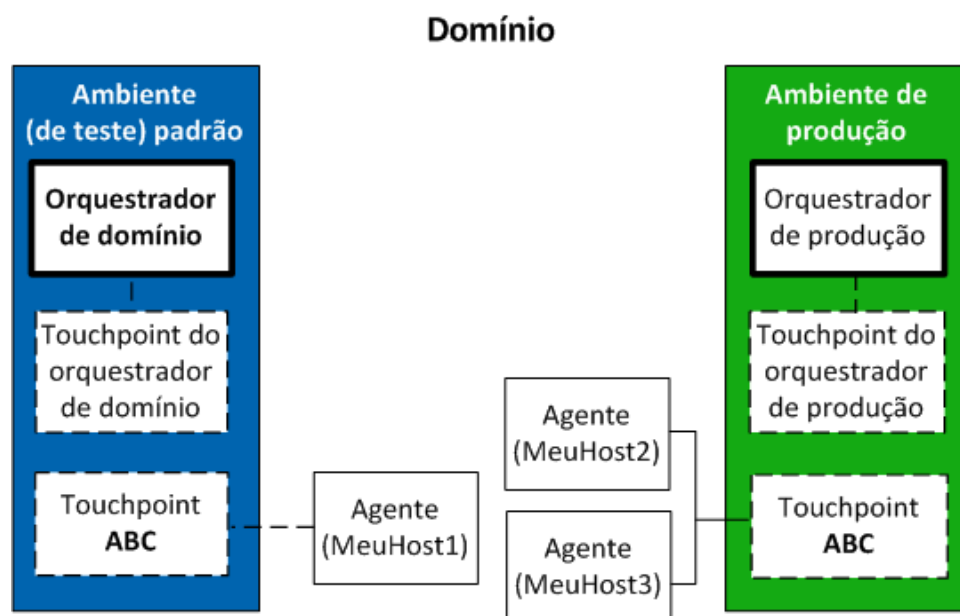
O ambiente padrão geralmente é dedicado à criação de processos automatizados. Os criadores de conteúdo desenvolvem processos que são executados no touchpoint do orquestrador de domínio. Quando o primeiro processo estiver pronto para fazer a transição para a produção, você cria um ambiente; um ambiente de produção é adicionado ao domínio.

A ilustração a seguir mostra o touchpoint como um bloco com uma borda tracejada. A ilustração mostra a associação entre o touchpoint e o orquestrador de domínio como uma linha tracejada.

Domínio

Ambiente (de teste) padrão

Orquestrador de domínio

Touchpoint do orquestrador de domínio

Um processo que é executado em um orquestrador pode incluir operadores que precisam usar outros hosts como destino. Esses destinos geralmente exigem que você instale um agente do CA Process Automation e, em seguida, associe touchpoints ao agente. Os criadores de conteúdo acessam o agente por meio do nome do seu touchpoint. Quando não é possível instalar um agente em um host de destino, os touchpoints do proxy são usados. Um *touchpoint do proxy* amplia o uso de touchpoints, de modo que os orquestradores possam executar operadores em um host remoto (ou seja, um host sem um agente instalado). Quando um touchpoint está configurado com uma conexão SSH entre o host do agente e um host remoto, é um touchpoint do proxy.

Para cada touchpoint com uma associação ao ambiente de criação, adicione um touchpoint com o mesmo nome e associe-o ao ambiente de produção. Assim, um operador que é executado no touchpoint ABC no ambiente de criação também pode ser executado em um touchpoint chamado touchpoint ABC no ambiente de produção. No ambiente de teste, o touchpoint pode ser associado a um único agente. Para oferecer suporte à alta disponibilidade no ambiente de produção, o touchpoint correspondente pode ser associado a dois agentes.

Mais informações:

Sobre a hierarquia de domínio, orquestradores e agentes (na página 151)

Cardinalidade das associações de componentes

Como um administrador do CA Process Automation, você cria o domínio instalando orquestradores e agentes. Para criar partições do domínio, crie ambientes, onde cada ambiente tem sua própria biblioteca. Você configura touchpoints para que os criadores de conteúdo especifiquem como destinos para os operadores. Clique na guia Configuração e abra a paleta Navegador de configuração para exibir essas entidades.

As regras a seguir regem a cardinalidade entre os pares de entidades que podem ter uma associação:

Domínio, Ambientes, Orquestradores e Agentes

Os orquestradores e agentes são componentes do software que estão *fisicamente* instalados em hosts. O domínio e os ambientes são entidades *lógicas*.

- Um sistema do CA Process Automation tem um único domínio.
- Quando um novo sistema do CA Process Automation é instalado, o domínio tem um ambiente padrão. O ambiente padrão contém o orquestrador de domínio.
- O domínio pode ter muitos ambientes. É possível adicionar ambientes para bibliotecas separadas. Por exemplo, é possível dedicar o ambiente padrão para criar e testar o novo conteúdo. Em seguida, você pode criar um ambiente de produção separado. Cada ambiente deve ter pelo menos um orquestrador.

  Observação: normalmente, um administrador exporta o conteúdo do ambiente padrão e, em seguida, o importa para o ambiente de produção. Você também pode transferir o conteúdo entre domínios.

- Um ambiente pode ter um ou mais orquestradores. Cada orquestrador é instalado em um host separado.

  Observação: um orquestrador pode ser *padrão* ou *agrupado*. Um orquestrador agrupado tem vários nós. Cada nó é instalado em um host separado. Um orquestrador é exibido como uma única entidade no Navegador de configuração, independentemente se for agrupado ou padrão (não agrupado).

- O domínio pode ter quantos agentes forem necessários. Os agentes são instalados em hosts e são independentes de ambientes.

Ambientes e Touchpoints

Ambientes e touchpoints são entidades *lógicas*.

- Cada touchpoint pertence a um ambiente.
- Cada ambiente pode ter muitos touchpoints.
- Para cada touchpoint usado em uma versão da release de um processo no ambiente de criação, deve haver um touchpoint com um nome idêntico no ambiente de produção. Isso permite que o processo não modificável seja executado no ambiente de produção.

Orquestradores e Touchpoints

Após instalar um orquestrador, você deve criar um touchpoint que associa o orquestrador a um ambiente específico. Os operadores em um processo usam como destino o touchpoint associado ao orquestrador. A associação do touchpoint determina o ambiente em que o processo é executado.

- O orquestrador de domínio possui um touchpoint predefinido.
- Cada orquestrador está associado a apenas um touchpoint.
- Um touchpoint associado a um orquestrador não pode ser associado a um agente. As associações touchpoint-orquestrador e touchpoint-agente são mutuamente exclusivas.
- Um operador será executado no touchpoint do orquestrador que executa o processo se o destino do operador estiver em branco.

Agentes e Touchpoints

Para tornar um agente disponível como um destino para um operador, associe o agente a um touchpoint, a um touchpoint do proxy ou a um grupo de hosts.

- É possível associar um agente a um ou mais touchpoints.
  - Ao associar um agente a um touchpoint, os operadores podem executá-lo diretamente em um host com um agente instalado, escolhendo o touchpoint como destino.
  - Ao associar um agente a vários touchpoints no mesmo host, os touchpoints normalmente têm como destino diferentes componentes no host. Por exemplo, pode-se definir um touchpoint para acessar um banco de dados e outro para acessar um produto de terceiros.
  - Cada operador em um processo é executado em um touchpoint, que pode ser associado a um operador, a um agente ou a vários agentes. Se o operador 1 for executado no Touchpoint-ABC no ambiente de criação, será executado em outro touchpoint chamado Touchpoint-ABC no ambiente de produção. Cada integrante deste par de touchpoints está associado a um ambiente diferente. Cada integrante do par de touchpoints pode ser associado ao mesmo agente ou a agentes diferentes. Esse tipo de associação fornece o mecanismo para definir processos que você pode migrar entre ambientes sem alterar as informações do host de destino.
- Você pode associar um touchpoint a um ou mais agentes. Você pode atribuir a mesma prioridade a vários agentes, ou atribuir uma prioridade diferente a cada agente.
  - Quando os agentes têm prioridades diferentes, os operadores são executados no agente com prioridade máxima. Se o agente de prioridade máxima não estiver disponível, os operadores serão executados em um agente disponível com uma prioridade mais baixa. Isso garante que um host de destino esteja disponível.
  - Quando vários agentes com a mesma prioridade estão associados a um touchpoint, os operadores são executados em um agente selecionado aleatoriamente. Isso promove o balanceamento de carga.
  - Um touchpoint associado a um orquestrador não pode ser associado a um agente.

Agentes, Touchpoints do proxy e hosts remotos

Um host remoto refere-se a um host que é o destino de um operador quando a instalação de um agente não é prática.

- É possível associar um agente a um ou mais touchpoints do proxy.
- Um *touchpoint do proxy* é um touchpoint que está configurado com uma conexão SSH com um host remoto. O host remoto normalmente não tem nenhum agente.
- Ao associar um agente a um touchpoint do proxy, os operadores em um processo podem ter como destino o touchpoint do proxy para a execução no host remoto.

Observação: um orquestrador pode distribuir a carga de trabalho para um host remoto sem passar por um agente usando o operador Executar o script SSH em um processo. O criador de conteúdo define os parâmetros de configuração (no operador) que especificam o endereço do host e as credenciais a serem usadas para SSH no host remoto e executar um script. Consulte o Guia de *Referência do Criador de Conteúdo* para obter detalhes sobre o operador Executar o script SSH.

Agentes, grupos de hosts e hosts remotos

Um *grupo de hosts* é um grupo de hosts remotos. Você normalmente configura grupos de hosts com um padrão de nome de host comum ou com uma sub-rede IPv4 expressa em notação CIDR.

- Você pode associar um agente a um ou mais grupos de hosts.
- Você pode associar um grupo de hosts a um ou mais agentes.
- Quando um agente for associado a um grupo de hosts, configure manualmente as conexões SSH. Configure uma conexão SSH a partir do host do agente para cada host remoto ao qual o grupo de hosts faz referência.
- Quando um agente está associado a um grupo de hosts, os operadores em um processo podem ser executados em um host remoto referenciado. Os operadores têm como destino o endereço IP ou FQDN do host remoto.

Observação: para a comunicação SSH não interativa com um host remoto, use um touchpoint do proxy ou um grupo de hosts. Para a comunicação SSH interativa com um host remoto, use o operador Executar o script SSH. Consulte o Guia de *Referência do Criador de Conteúdo* para obter detalhes sobre o operador Executar o script SSH.

Segurança

Como um administrador, suas preocupações de segurança do CA Process Automation podem incluir:

- Proteger o aplicativo do CA Process Automation (na página 39).
- Suspender ou desativar uma conta de usuário (na página 40).
- Proteger a transferência de dados com códigos fortes (na página 41).
- Proteger a transferência de dados entre o CA Process Automation e o CA EEM (na página 41).

Mais informações:

Administrar a segurança básica do CA EEM (na página 43)

Protegendo o aplicativo do CA Process Automation

Um aspecto da proteção do aplicativo é evitar que usuários não autorizados efetuem logon. Outro é limitar o uso da funcionalidade de acordo com a função do usuário conectado. A proteção do aplicativo inclui os seguintes mecanismos:

Autenticação

O produto usa o CA EEM para autenticar usuários no logon. O CA EEM compara as credenciais que os usuários digitam para efetuar logon com as combinações de nome de usuário e senha em suas contas de usuário. O usuário poderá efetuar logon apenas se o CA EEM encontrar uma correspondência.

Os administradores podem ajudar a proteger o produto de logons não autorizados ao solicitar que os usuários alterem as senhas periodicamente e suspender ou desativar as contas padrão. Para obter mais informações, consulte os tópicos:

- Alterar sua própria senha no CA EEM (na página 47)
- Suspender ou desativar uma conta de usuário (na página 40)

Autorização e segurança com base em funções

O produto usa o CA EEM para autorizar usuários conectados. O CA EEM permite que os usuários executem tarefas apenas nas partes da interface de usuário para as quais estão autorizados. A autorização para os grupos PAMAdmins, Criadores e Usuários de produção é definida por padrão. Os usuários adicionados a esses grupos herdam a autorização.

Os administradores podem definir a segurança com base em funções, para que os usuários que pertencem a diferentes grupos acessem apenas as partes do produto necessárias para a função que executam. Os administradores também podem usar as diretivas do CA EEM para atribuir usuários confiáveis a atividades para as quais o uso indevido podem causar grandes danos. Esse aspecto do controle de acesso é uma consideração separada da função do grupo para a qual usuários individuais são atribuídos.

Mais informações:

Autenticação e autorização de usuários no modo FIPS (na página 379)

Suspendendo ou desativando uma conta de usuário

É possível suspender ou desativar uma conta de usuário nos seguintes casos:

- O usuário não precisa mais acesso ao CA Process Automation, mas o registro do usuário deve ser mantido para fins de auditoria.
- É necessário ter motivos para impedir que o usuário acesse o CA Process Automation temporariamente ou permanentemente.
- As credenciais predefinidas disponibilizadas durante a instalação representam agora uma ameaça à segurança interna. Como as credenciais do pamadmin e do pamuser estão documentadas, é uma boa prática torná-las disponíveis após terem cumprido sua finalidade.

Siga estas etapas:

1. Efetue logon em CA EEM.
2. Clique em Gerenciar identidades.
3. Em Pesquisar usuários, selecione Detalhes do usuário do aplicativo e clique em Ir.
4. Clique no nome do usuário de destino.
5. Role para a área Autenticação e execute uma das seguintes ações:
   - Clique em Suspenso
   - Clique em Desativar data, selecione a data que será desativada e clique em OK.
6. Clique em Salvar.

Observação: também é possível reverter a suspensão ou ativar uma conta desativada. É possível usar o recurso ativar/desativar para adiar a disponibilidade de uma nova conta para o tempo que você especificar.

Protegendo a transferência de dados com códigos fortes

Quando os componentes CA Process Automation são instalados em máquinas virtuais Java, as JVMs como a Java 6 permitem codificações Média e Baixa nas comunicações com os agentes. Para proteger essas comunicações, adicione valores de código fortes ao arquivo de propriedades Oasis.Config no seguinte diretório:

install_dir\server/c2o\config\

As propriedades a seguir estão relacionadas a codificações usadas em comunicação SSL:

jboss.ssl.ciphers

Especifica uma lista de codificações, separada por vírgula, a ser usada para a comunicação SSL entre o Orquestrador de domínio e os clientes, tais como navegadores e serviços web. A lista de códigos pode variar de acordo com o sistema operacional e a JVM que estiverem no host. O exemplo a seguir mostra uma especificação típica de codificações fortes de JBoss:

```
jboss.ssl.ciphers=SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DS
S_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE
_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_
RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA
```

jetty.ssl.ciphers

Especifica uma lista de codificações separada por vírgulas, a ser usada para a comunicação SSL com agentes. O produto adiciona essa propriedade aos agentes durante a instalação silenciosa. O exemplo a seguir mostra uma especificação típica de codificações fortes de Jetty:

```
jetty.ssl.ciphers=SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA
_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA
```

Proteger a transferência de dados entre o CA Process Automation e o CA EEM

O CA Process Automation usa a criptografia para proteger dados armazenados e transmitidos. Se o modo FIPS do CA EEM for definido como ativado, o CA Process Automation protege os dados armazenados e transmitidos com os módulos FIPS-140-2 criptográficos validados.

Tipos de autenticação

O CA EEM autentica e autoriza todos os usuários que navegam para o CA Process Automation. O CA EEM pode autenticar os usuários de uma das seguintes maneiras:

- Usando as credenciais que os usuários inserem em uma caixa de diálogo de logon com base em formulário.
- Usando o protocolo de NTLM, se a autenticação de passagem NTLM estiver configurada. Normalmente, esse recurso é selecionado quando o CA EEM está configurado para usar o Microsoft Active Directory como um diretório externo. As credenciais do usuário são carregadas automaticamente no CA EEM para essa configuração.

Quando um usuário navega para o CA Process Automation, o orquestrador determina o tipo de autenticação a ser usado:

Com base em formulário

A página de logon do CA Process Automation é exibida. O usuário insere as credenciais e o processo de logon é iniciado.

NTLM

O protocolo NTLM autentica o usuário para o servidor do CA EEM, e a página Início é exibida.

Capítulo 3: Administrar a segurança básica do CA EEM

Quando você instala o CA Process Automation ou a atualização, o CA Process Automation é registrado com o CA EEM. O CA EEM fornece gerenciamento de diretiva de acesso, serviços de autenticação e autorização para muitos produtos CA Technologies. A administração de segurança varia de acordo com o fato de você estar configurando a segurança pela primeira vez ou atualizando o CA Process Automation. Se você estiver atualizando, os requisitos de segurança dependerão do fato de você já ter usado o CA EEM ou LDAP para autenticação de usuário. Se você for um novo usuário ou estiver atualizando, se planeja carregar contas de usuário de um servidor de diretório externo para o CA EEM, um conjunto de procedimentos separados é obrigatório.

Este capítulo aborda o uso do CA EEM para atribuir a cada usuário uma das quatro funções padrão, se você estiver criando contas de usuário, tiver contas de usuário existentes, ou estiver carregando contas de usuários de um diretório externo.

Consulte o tópico Administrar a segurança avançada do CA EEM (na página 73) se estiver criando funções e diretivas personalizadas.

Esta seção contém os seguintes tópicos:

Determinar o processo para conseguir acesso com base em função

A administração de segurança com o CA EEM varia para os seguintes cenários:

- Instalação nova ou de atualização com um servidor de diretório referenciado: você configurou o CA EEM de tal forma que a autenticação seja baseada nas credenciais que são carregadas no CA EEM como contas de usuário global de um armazenamento de usuário externo. Você está pronto para atribuir um grupo de aplicativos a cada usuário global que reflete a função executada no CA Process Automation.
- Nova instalação com um CA EEM local: você está pronto para definir os usuários do CA Process Automation no CA EEM.
- Instalação de atualização, onde anteriormente você usava o CA EEM: é possível atualizar contas de usuário para usuários que criam processos ou que usem processos transicionados para o ambiente de produção. Abra cada conta e selecione um dos novos grupos de aplicativos: criadores ou usuários de produção.
- Instalação de atualização, onde anteriormente você usava o Microsoft Active Directory ou servidor LDAP semelhante. Você está pronto para criar contas de usuários existentes no CA EEM. Você pode atribuir um grupo padrão a usuários ou pode criar grupos personalizados que permitam manter as funções usadas com o AD.

Determinar processo para conseguir acesso com base em função

Administrador do CA EEM

Usar armazenamento de usuários externo?
Sim
Gerenciar acesso a contas de usuários de referência
Não
Novo?
Sim
Criar contas de usuário com funções padrão
Não
Já usava o CA EEM?
Sim
Atualizar contas de usuário com funções padrão
Não
Já usava o AD?
Sim
Manter direitos do AD?
Sim
Criar contas de usuário com funções personalizadas do AD
Não

Com base no resultado do gráfico de decisão, consulte a seção apropriada:

- Gerenciar acesso a contas de usuários de referência (na página 62).
- Criar contas de usuário com funções padrão (na página 55).
- Atualizar contas de usuário com funções padrão (na página 61).
- Criar contas de usuário com funções personalizadas do AD.

  Consulte o tópico Como realizar a transição de funções utilizadas no Active Directory para o CA EEM (na página 114).

Navegue até o CA EEM e efetue logon.

Para gerenciar usuários, grupos de usuários e diretivas que concedem permissões no CA Process Automation, efetue logon no aplicativo configurado no CA EEM.

Siga estas etapas:

1. Vá até o CA EEM usado pelo CA Process Automation. Use o seguinte URL:

   `https://`*`nome_do_host`*`:5250/spin/eiam`

   A caixa de diálogo CA Embedded Entitlements Manager é exibida.

2. Na lista suspensa Aplicativo, selecione o nome configurado na instalação no campo Nome do aplicativo do EEM.

   Observação: o nome padrão é Process Automation.

3. Digite um dos seguintes conjuntos de credenciais:

   - Digite **EiamAdmin** e a senha do administrador do CA EEM que foi estabelecida durante o processo de instalação.
   - Digite seu nome de usuário e a senha se o administrador do CA EEM tiver concedido a você acesso ao CA EEM. O administrador do CA EEM pode conceder acesso ao CA EEM para administradores selecionados (na página 75).

4. Clique em Efetuar logon.

Usar o CA EEM para alterar sua senha do CA Process Automation

O administrador geralmente atribui uma senha temporária ao configurar contas de usuário para o armazenamento de usuários interno. Todos os usuários do CA Process Automation com contas de usuário criadas no CA EEM podem alterar essa senha antes de efetuar logon no CA Process Automation. Em seguida, você poderá alterar sua senha do CA Process Automation no intervalo definido pelas diretivas de senha.

Observação: esse recurso não se aplica quando o CA EEM fizer referência a contas de usuários de um armazenamento de usuários externo, como o Microsoft Active Directory. Nesse caso, mantenha sua senha no diretório referenciado.

Use o CA EEM para alterar sua senha do CA Process Automation.

Siga estas etapas:

1. Abra um navegador e digite o URL para o servidor do CA EEM que o CA Process Automation utiliza. Por exemplo:
   `https://`*`nome_do_host_ou_endereço_IP`***`:5250/spin/eiam/`**

   Para identificar o nome do host ou o endereço IP do CA EEM que o CA Process Automation utiliza, consulte o campo Servidor de back-end do CA EEM, na guia Configuração e na subguia Segurança do CA Process Automation.

2. Faça logon no CA Embedded Entitlements Manager (CA EEM) na caixa de diálogo Efetuar logon:

   a. Para Aplicativo, selecione <Global>.

   b. Exclua EiamAdmin se esse nome padrão for exibido no campo Nome do usuário.

   c. Digite seu nome de usuário e senha do CA Process Automation.

   d. Clique em Efetuar logon.

3. Em Autoadministração, clique em Alterar senha.

4. Redefinir sua senha:

   a. Digite seu nome de usuário do CA Process Automation e a senha antiga.

   b. Em seguida, digite a nova senha nos campos Nova senha e Confirmar senha.

   c. Clique em OK.

   O CA Process Automation aceita as credenciais atualizadas quando você efetua logon.

Acesso à configuração com base em função

O acesso com base em funções é implementado no CA EEM, onde PAMAdmins (para administradores), criadores e usuários de produção formam três grupos específicos do aplicativo. Cada grupo recebe permissões para acessar somente a funcionalidade relevante à respectiva função. O quarto grupo padrão, PAMUsers, pode ser usado como a base para grupos personalizados, quando aplicável.

PAMAdmins (Administradores)

Os administradores têm acesso total à guia Configuração. Os administradores definem as configurações em todos os níveis da hierarquia de domínio. As paletas Instalação e Gerenciar recursos de usuário estão presentes na guia Configuração somente para os usuários que são administradores.

Criadores

O CA EEM concede aos usuários no grupo Criadores a capacidade de exibir o navegador de configuração e as definições de configuração na guia Configuração. Os criadores de conteúdo podem examinar se agentes específicos falharam ou se uma categoria específica de operadores está desativada em um determinado touchpoint.

Usuários de produção

O CA EEM concede aos usuários no grupo Usuários de produção a capacidade de exibir a guia Configuração.

Grupos padrão e credenciais de usuário padrão

O CA EEM fornece quatro grupos padrão para o CA Process Automation. Cada grupo tem um usuário padrão. Você pode experimentar o CA Process Automation apresentado aos integrantes de cada um deles, efetuando logon no CA Process Automation como usuário padrão. As descrições e as credenciais de alto nível para usuários padrão são apresentadas a seguir:

PAMAdmins

O grupo PAMAdmins recebe permissões totais no CA Process Automation. É possível atribuir esse grupo a todos os administradores.

Credenciais de usuário padrão

Nome de usuário: pamadmin

Senha: pamadmin

Criadores

O grupo Criadores recebe permissões que normalmente são suficientes para os usuários que criam processos automatizados.

Credenciais de usuário padrão

Nome de usuário: pamdesigner

Senha: pamdesigner

Usuários de produção

O grupo Usuários de produção recebe permissões suficientes para os usuários que interagem com processos automatizados no ambiente de produção.

Credenciais de usuário padrão

Nome de usuário: pamproduser

Senha: pamproduser

PAMUsers

O grupo PAMUsers padrão recebe permissões mínimas. O administrador do CA EEM podem usar este grupo como base para grupos personalizados. Este grupo concede a capacidade de efetuar logon no CA Process Automation, examinar relatórios e exibir o estado das operações.

Credenciais de usuário padrão

Nome de usuário: pamuser

Senha: pamuser

As descrições detalhadas das permissões são apresentadas seguir:

- Permissões do grupo PAMAdmins (na página 50).
- Permissões do grupo Criadores (na página 51).
- Permissões do grupo Usuários de produção (na página 53).
- Permissões do grupo PAMUsers (na página 54).

A edição das funções padrão ou a criação de funções personalizadas é um recurso avançado.

Permissões do grupo PAMAdmins

As diretivas do CA EEM que o CA Process Automation fornece concede todas as permissões para o grupo de aplicativos PAMAdmins. Atribua esse grupo a administradores que precisam de acesso completo ao CA Process Automation. O grupo PAMAdmins fornece o seguinte acesso de nível de guias:

Página inicial

Os administradores do grupo PAMAdmins têm acesso completo à guia Início. O acesso completo consiste em permissão para efetuar logon no CA Process Automation e usar a guia Início (diretiva de logon do usuário PAM40).

Biblioteca

Os administradores do grupo PAMAdmins têm acesso completo à guia Biblioteca, que consiste nas seguintes permissões:

- Exibir a guia Biblioteca (diretiva de navegador da biblioteca PAM40).
- Controlar as pastas da biblioteca e seu conteúdo (direitos de Environment_Library_Admin na diretiva de ambiente PAM40).
- Configurar as variáveis comuns a um grupo de operadores personalizados e publicar a configuração do grupo na paleta Navegador de configuração da guia Módulos (diretiva de configuração do grupo PAM40).

Designer

Os administradores do grupo PAMAdmins têm acesso completo à guia Criador, que consiste nas seguintes permissões:

- Exibir a guia Criador (diretiva de criador).
- Direitos totais na guia Criador (direitos de Environment_Library_Admin na diretiva de ambiente PAM40).

Operações

Os administradores do grupo PAMAdmins têm acesso completo à guia Operações, que consiste nas seguintes permissões:

- Exibir todas as paletas na guia Operações (diretiva de operações PAM40).
- Permissões totais (direitos de Environment_Library_Admin na diretiva de ambiente PAM40).

Configuração

Os administradores do grupo PAMAdmins têm acesso completo à guia Configuração, que consiste nas seguintes permissões:

- Exibir todas as paletas da paleta Navegador de configuração (diretiva de configuração PAM40).
- Configurar no nível de domínio ou executar uma tarefa que requer o bloqueio do domínio (diretiva de domínio PAM40).
- Configurar no nível de Ambiente ou concluir uma tarefa que requer o bloqueio de um ambiente (direitos Environment_Config_Admin na diretiva de ambiente PAM40).
- Instalar agentes ou orquestradores (diretiva de configuração PAM40).
- Gerenciar recursos de usuário (diretiva de configuração PAM40).

Relatórios

Os administradores do grupo PAMAdmins têm acesso completo à guia Relatórios. O acesso completo consiste em permissões para exibir a guia Relatórios, gerar relatórios e adicionar novos relatórios (diretiva de relatórios PAM40).

Permissões do grupo Criadores

Por padrão, o grupo de aplicativos Criadores contém permissões necessárias para os usuários no ambiente de criação. O grupo Criadores fornece o seguinte acesso de nível de guias:

Página inicial

Os usuários do grupo Criadores podem efetuar logon no CA Process Automation e usar a guia Início (diretiva de logon do usuário PAM40).

Biblioteca

Os usuários do grupo Criadores têm o seguinte acesso à guia Biblioteca:

- Exibir a guia Biblioteca (diretiva de navegador da biblioteca PAM40).
- Ler a guia Biblioteca, incluindo permissão para exibir, exportar e pesquisar objetos de automação (diretiva de ambiente PAM40).
- Controlar (exibir, navegar, editar, excluir, criar) pastas na guia Biblioteca e controlar todos os objetos de automação em seus respectivos editores (diretiva de objeto PAM40).

Designer

Os usuários do grupo Criadores têm o seguinte acesso à guia Criador:

- Exibir a guia Criador (diretiva de criador PAM40).
- Criar processos automatizados e controlar (exibir, navegar, editar, excluir e criar) todos os objetos de automação em seus respectivos editores. A guia Criador é o editor de objetos de automação de processos (diretiva de objeto PAM40).

Operações

Os usuários do grupo Criadores têm o seguinte acesso à guia Operações:

- Exibir todas as paletas na guia Operações (diretiva de operações PAM40).
- Controlar as programações exibidas na guia Operações (diretiva de programação PAM40).
- Inspecionar e modificar o objeto de automação de conjunto de dados (diretiva de conjunto de dados PAM40).
- Controlar, iniciar e monitorar o objeto de automação de processos (diretiva de processo PAM40).
- Controlar o objeto de automação de recursos (diretiva de recursos PAM40).
- Iniciar e retirar da fila a diretiva de formulário de solicitação inicial (diretiva de formulário de solicitação inicial PAM40).
- Exibir a versão da release de um pacote de conteúdo importado e exibir os objetos contidos nele.

Configuração

Os usuários do grupo Criadores podem exibir as guias de qualquer nó que selecionarem na paleta Navegador de configuração (diretiva de configuração PAM40).

Relatórios

Os usuários do grupo Criadores podem exibir a guia Relatórios, gerar relatórios e adicionar relatórios. O grupo Criadores tem como base o grupo PAMUsers, que também tem essas permissões.

Permissões do grupo Usuários de produção

Por padrão, o grupo de aplicativos Usuários de produção contém permissões necessárias para os usuários em um ambiente de produção. O grupo Usuários de produção fornece o seguinte acesso de nível de guias:

Página inicial

Os usuários atribuídos ao grupo Usuários de produção têm acesso para efetuar logon no CA Process Automation e usar a guia Início (diretiva de logon do usuário PAM40).

Biblioteca

Os usuários do grupo Usuários de produção têm o seguinte acesso à guia Biblioteca:

- Exibir a guia Biblioteca (diretiva de navegador da biblioteca PAM40).
- Ler a guia Biblioteca (diretiva de ambiente PAM40, que é um pré-requisito para a diretiva de objeto PAM40).
- Navegar pela estrutura de pastas da guia Biblioteca e exibir os objetos de automação listados em cada pasta (diretiva de objeto PAM40).

Operações

Os usuários do grupo Usuários de produção têm o seguinte acesso à guia Operações:

- Exibir todas as paletas na guia Operações (diretiva de operações PAM40).
- Controlar as programações exibidas na guia Operações (diretiva de programação PAM40).
- Inspecionar qualquer conjunto de dados exibido na paleta Conjunto de dados da guia Operações (diretiva de conjunto de dados PAM40).
- Monitorar ou iniciar qualquer processo exibido na guia Operações (diretiva de processo PAM40).
- Iniciar e retirar da fila o formulário de solicitação inicial exibido na guia Operações (diretiva de formulário de solicitação inicial PAM40).
- Exibir a versão da release de um pacote de conteúdo importado e exibir os objetos contidos nele.

Configuração

Os usuários do grupo Usuários de produção podem exibir as guias de qualquer nó selecionado na paleta Navegador de configuração (diretiva de configuração PAM40).

Relatórios

Os usuários do grupo Usuários de produção podem exibir a guia Relatórios, gerar relatórios e adicionar relatórios (diretiva de relatórios PAM40).

Permissões do grupo PAMUsers

Por padrão, o grupo de aplicativos PAMUsers contém permissões básicas. Use esse grupo para complementar os grupos personalizados que você criar para o acesso refinado com base em funções. O grupo PAMUsers fornece o seguinte acesso de nível de guias:

Página inicial

Os usuários do grupo PAMUsers podem efetuar logon no CA Process Automation e usar a guia Início (diretiva de logon do usuário PAM40).

Biblioteca

Os usuários do grupo PAMUsers têm o seguinte acesso à guia Biblioteca:

- Exibir a guia Biblioteca (diretiva de navegador da biblioteca PAM40).
- Ler a guia Biblioteca (diretiva de ambiente PAM40).

Operações

Os usuários do grupo PAMUsers podem exibir a guia Operações (diretiva de operações PAM40).

Relatórios

Os usuários do grupo PAMUsers podem exibir a guia Relatórios, gerar relatórios e adicionar relatórios (diretiva de relatórios PAM40).

Criar contas de usuário com funções padrão

Quando o instalador configura o CA EEM para usar o armazenamento de usuários interno, o administrador do CA EEM cria uma conta de usuário para cada usuário do CA Process Automation. Essas contas de usuário são usadas para autenticar os usuários quando eles efetuam logon no CA Process Automation. Para autorizar esses usuários a acessar os recursos necessários para suas funções, o administrador do CA EEM atribui o grupo padrão apropriado para cada conta de usuário.

A ilustração a seguir mostra como criar contas de usuário com funções padrão. As linhas tracejadas indicam as tarefas que você executa fora do CA Process Automation.

Criar contas de usuário com funções padrão

Administrador do CA EEM

Ir até o CA EEM e efetuar logon

Verificar as permissões concedidas aos grupos padrão

Aceitar os grupos padrão?

Não

Criar diretivas e grupos personalizados

Criar contas de usuário e atribuir grupos personalizados

Sim

Identificar os usuários que configuram o PAM ou gerenciam a criação ou as operações

Criar contas com acesso completo (PAMAdmins)

Identificar os usuários que automatizam os processos

Criar contas com acesso de criador (Criadores)

Identificar os usuários que trabalham com os processos (operações)

Criar contas com acesso a operações (Usuários em produção)

Identificar os usuários que precisam de acesso básico

Criar contas com acesso básico (PAMUsers)

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Verificar permissões para grupos padrão.

- Permissões do grupo PAMAdmins (na página 50)
- Permissões do grupo Criadores (na página 51)
- Permissões do grupo Usuários de produção (na página 53)
- Permissões do grupo PAMUsers (na página 54)

3. Criar contas de usuário para administradores (na página 56).
4. Cria contas de usuário para criadores (na página 57).
5. Criar contas de usuário para usuários de produção (na página 58).
6. Apresentar novos usuários ao CA Process Automation (na página 60).

Crie contas de usuário para administradores

Os administradores precisam de acesso completo a todos os recursos do CA Process Automation. Para conceder esse acesso, associe as contas de usuário de administradores com o grupo PAMAdmins.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.
3. Na paleta Usuários, clique no ícone ao lado de Usuários.

   A página Novo usuário é aberta.
4. No campo Nome do usuário, digite a ID de usuário para atribuir à conta de usuário.

   O usuário digita esse valor no campo Nome do usuário no momento do logon.
5. Clique em Adicionar detalhes do usuário do aplicativo.

   O painel é atualizado para mostrar a seção Associação ao grupo de aplicativos.
6. Selecione PAMAdmins em Grupos de usuários disponíveis e clique em > para movê-lo para Grupos de usuários selecionados.
7. Insira os detalhes do usuário global.
   a. Digite o nome nos campos Nome e Sobrenome.

      A barra de títulos exibe esses valores quando o usuário efetua logon no CA Process Automation.

   b. Preencha os outros campos na área Geral conforme apropriado.
8. (Opcional) Se você usar o CA Process Automation com outro produto da CA Technologies que usa esse CA EEM, preencha a seção Associação a grupo global.

9. Forneça informações de autenticação temporária para essa conta de usuário:
   a. Selecione Alterar senha no próximo logon.
   b. Digite uma senha temporária no campo Nova senha.
   c. Digite a mesma senha temporária no campo Confirmar senha.
10. (Opcional) Preencha os campos restantes na página Novo usuário.
11. Clique em Salvar e, em seguida, em Fechar.
12. (Opcional) Clique em Logoff.

Criar contas de usuário para criadores

Criar uma conta de usuário para cada criador que exige acesso a objetos de automação no CA Process Automation. Os objetos de automação são usados para automatizar processos.

Siga estas etapas:

1. Navegue até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.
3. Clique em Novo usuário.

   A página Novo usuário é exibida.
4. Digite a ID de usuário para atribuir à conta de usuário no campo Nome.
5. Clique em Adicionar detalhes do usuário do aplicativo.
6. Selecione Criadores em Grupos de usuários disponíveis e clique em> para movê-lo para Grupos de usuários selecionados.
7. Insira os detalhes do usuário global.
8. Digite e confirme a senha.

   Os usuários podem alterar sua senha no CA EEM.
9. (Opcional) Preencha os campos restantes na página Novo usuário.
10. Clique em Salvar e, em seguida, clique em Fechar.
11. Clique em Logoff.

Criar contas de usuário para usuários de produção

Criar uma conta de usuário para cada usuário de produção que exige acesso ao CA Process Automation para monitorar e interagir com processos automatizados.

Siga estas etapas:

1. Navegue até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.
3. Clique em Novo usuário.

   A página Novo usuário é exibida.
4. Digite a ID de usuário para atribuir à conta de usuário no campo Nome.
5. Clique em Adicionar detalhes do usuário do aplicativo.
6. Selecione Usuários de produção em Grupos de usuários disponíveis e clique em> para mover essa opção para Grupos de usuários selecionados.
7. Insira os detalhes do usuário global.
8. Digite e confirme a senha.

   Os usuários podem alterar sua senha no CA EEM.
9. (Opcional) Preencha os campos restantes na página Novo usuário.
10. Clique em Salvar e, em seguida, clique em Fechar.
11. Clique em Logoff.

Criar contas de usuário com acesso básico

PAMUsers é um grupo padrão que concede o uso das guias Início e Relatórios e concede acesso somente leitura às guias Biblioteca e Operações. Um usuário com acesso somente PAMUsers pode se familiarizar com o produto, mas não pode criar nem configurar objetos.

Use esse grupo como a base para grupos personalizados.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.
3. Clique em Novo usuário.
4. Digite a ID de usuário para atribuir à conta de usuário no campo Nome.
5. Clique em Adicionar detalhes do usuário do aplicativo e clique em > para mover PAMUsers para os Grupos de usuários selecionados.

6. Insira os detalhes do usuário global.
7. Digite e confirme a senha.

   Os usuários podem efetuar logon no CA EEM com suas credenciais do CA Process Automation e alterar suas senhas.
8. (Opcional) Preencha os campos restantes na página Novo usuário.
9. Clique em Salvar e em Fechar.
10. Clique em Logoff.

Introdução de novos usuários ao CA Process Automation

Para ajudar os novos usuários a se tornarem produtivos, forneça as seguintes informações:

Informações de acesso

- O URL do CA Process Automation. Isso poderia ser o URL do orquestrador de domínio ou o URL para o balanceador de carga do orquestrador de domínio. Opcionalmente, é possível ir até o URL de qualquer orquestrador especificado.
- Informações de logon. Os usuários efetuam logon com o nome de usuário e a senha configurada em sua conta de usuário do CA EEM.
- O URL do CA EEM. Os usuários efetuam logon com o nome de usuário e a senha que você atribuiu a eles e, em seguida, definem uma nova senha.

  Observação: se o CA EEM fizer referência a um ou mais Microsoft Active Directories externos, os usuários não precisarão efetuar logon no CA EEM. As senhas são mantidas pelo AD.

Acesso aos recursos para entrar em ação rapidamente

- Recomendamos que os usuários completem os tutoriais do CA Process Automation que podem ser acessados na guia Início.
- Mostre aos usuários que eles podem acessar a biblioteca, selecionando a opção Biblioteca no link AJUDA na barra de ferramentas. Os usuários podem acessar os guias relativos à sua função a partir da biblioteca.

  As guias para cada grupo de aplicativos (função) são:

  PAMAdmins

  Notas da Versão

  Guia de Instalação

  Guia de Administrador de Conteúdo

  Referência de interface de usuário

  Criadores

  Guia do Criador de Conteúdo

  Referência do Criador de Conteúdo

  Referência da API de serviços web

  Guia de Produção do Usuário

  Referência de interface de usuário

  Usuários de produção

  Guia de Produção do Usuário

  Referência de interface de usuário

Atualizar contas de usuário com funções padrão

A atualização de usuários que foram atribuídos anteriormente ao PAMAdmins (ou ITPAMAdmins) como o grupo de criadores ou usuários de produção pode melhorar a segurança. Se você for e estiver atualizando o usuário, considere a possibilidade de atribuir os seguintes grupos padrão aos usuários que executam as seguintes funções:

- Criadores
- Usuários de produção

Observação: se você já tiver atribuído PAMUsers (ou ITPAMUsers) a contas de usuário de pessoas que trabalharam com Listas de tarefas, Exibição de processos padrão ou Solicitações de usuário, reatribua o grupo Usuários de produção a essas contas.

Siga estas etapas:

1. Navegue até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.
3. Expanda a paleta Pesquisar usuários, selecione Usuários do aplicativo, insira os critérios a seguir e clique em Ir.
   - Atributo: Associação ao grupo
   - Operador: LIKE
   - Valor: PAMAdmins

   A lista de contas de usuário atualmente atribuída ao grupo PAMAdmins é exibida.
4. Clique no nome de um usuário que é um criador ou um usuário de produção.

   A conta de usuário selecionada é aberta.
5. Selecione PAMAdmins nos Grupos de usuários selecionados e clique na seta para a esquerda

   O grupo selecionado é removido de Grupos de usuários selecionados.
6. Selecione o grupo aplicável em Grupos de usuários disponíveis e clique em > para movê-lo a Grupos de usuários selecionados.
   - Para criadores de conteúdo, selecione Criadores.
   - Para usuários de produção, selecione Usuários de produção.
7. Clique em Salvar e, em seguida, clique em Fechar.
8. Clique em Logoff.

Gerenciar acesso a contas de usuários de referência

Se você fizer referência a um armazenamento de usuários externos durante a instalação do CA EEM, os grupos globais e as contas de usuário serão carregados automaticamente no CA EEM. O CA Process Automation permite o carregamento de até 10.000 contas com um parâmetro configurável que estende a definição do CA EEM de 2.000. Para obter informações sobre como personalizar essa configuração, consulte o tópico Definir o número máximo de usuários e grupos do CA EEM (na página 63).

As contas de usuário de um armazenamento de usuários externo referenciado são carregadas como somente leitura. Se um novo usuário precisar de uma conta, crie-a no armazenamento de usuários externos. O novo registro é carregado automaticamente. É possível fornecer acesso ao CA Process Automation no nível de grupo global ou de usuário global.

Você configura o CA EEM para conceder acesso ao CA Process Automation e a seus componentes, mas o armazenamento de usuário referenciado gerencia a autenticação. Para efetuar logon no CA Process Automation, os usuários globais com acesso de logon usam o nome de usuário e a senha (ou o nome da entidade principal e a senha) no armazenamento de usuários referenciado.

Observação: não é possível usar o CA EEM para atualizar os registros de usuário armazenados em um armazenamento de usuário externo.

Para gerenciar o acesso de usuários com contas armazenadas em um armazenamento de usuário externo, considere as abordagens a seguir.

- Adicione um grupo de aplicativos a cada conta de usuário global.

  Pesquise cada usuário global pelo nome. Atribua um dos grupos de aplicativos padrão (PAMAdmins, Criador, Usuários de produção ou PAMUsers) ou um grupo personalizado à conta de usuário global. Também é possível criar grupos globais e adicionar os usuários globais selecionados a esses grupos.

  Importante: Sempre digite os critérios ao pesquisar para evitar a exibição de todas as entradas em um armazenamento de usuários externos.

- Adicione um grupo global às diretivas de acesso do CA Process Automation e selecione as ações a serem concedidas.

  Em especial, adicione o grupo global às diretivas predefinidas para conceder o acesso desejado a todos os usuários no grupo. Por exemplo, adicione o grupo global à diretiva de logon de usuário PAM40 para permitir que todos os usuários globais desse grupo efetuem logon no CA Process Automation. Para conceder acesso à guia Criador, adicione o grupo à diretiva Criador PAM40.

- Crie um grupo dinâmico composto de usuários globais ou grupos globais selecionados. É possível adicionar grupos de aplicativos personalizados a um grupo dinâmico.
- Siga o procedimento documentado no tópico Integrar o Active Directory ao CA EEM.

  Esse procedimento concede a todos os usuários do seu AD acesso total ao CA Process Automation sem nenhuma configuração no CA EEM. Embora seja fácil de implementar, ele não possui a segurança do acesso com base em funções.

Importante: para servidores LDAP de terceiros, configure o seguinte parâmetro no nível de contexto ou=system:

```
ou = Grupos globais
```

Definir o número máximo de usuários e grupos do CA EEM

Antes de integrar um grande armazenamento de usuários referenciado, verifique se o armazenamento contém mais de 10.000 usuários e grupos. O valor padrão de eem.max.search.size (10.000) é o limite para o número de usuários e grupos que o CA Embedded Entitlements Manager pode aceitar durante a transferência. O padrão do CA Process Automation (10.000) estende o padrão do CA EEM (2.000).

Aumente o valor de eem.max.search.size se a seguinte mensagem for exibida quando você procurar por usuários disponíveis sem definir critérios de pesquisa:

```
O limite máximo de pesquisa foi excedido.
```

Para substituir o limite padrão no arquivo OasisConfig.properties, defina o seguinte parâmetro com um novo valor:

```
eem.max.search.size = 10000
```

Se você estiver integrando um grande diretório referenciado, defina o valor como mais de 20.000.

Siga estas etapas:

1. Efetue logon como administrador no servidor onde o orquestrador de domínio estiver instalado.
2. Vá até a seguinte pasta:

   install_dir/server/c2o/.config

   install_dir

   Refere-se ao caminho em que o orquestrador de domínio está instalado.
3. Abra o arquivo OasisConfig.properties com um editor de texto.

4. Use a opção Localizar para encontrar o parâmetro eem.max.search.size.
5. Altere o valor de 10000 para um valor apropriado.
6. Salve o arquivo e feche o editor de texto.
7. Reinicie o orquestrador:
   a. Interrompa o orquestrador (na página 193).
   b. Inicie o orquestrador (na página 194).

Pesquisar identidades correspondentes a critérios específicos

Ao fazer referência a um grande armazenamento de usuários externo, especifique os critérios de pesquisa. Os critérios de pesquisa limitam os registros retornados de conta de usuário global ao necessário ou a um subconjunto relevante. Por exemplo, especifique **Nome COMO John** para recuperar os nomes de todos os usuários com o nome John.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique em Gerenciar identidades.
3. Selecione Usuários globais no painel Pesquisar usuários.
4. Revise a lista suspensa Atributo e determine se algum atributo listado tem um valor para os usuários que você planeja pesquisar.
   - Em caso afirmativo, selecione um ou mais atributos aplicáveis. Por exemplo, selecione Nome e Sobrenome.
   - Caso contrário, selecione a elipse (...) e digite o nome do atributo para pesquisa.
5. Selecione o operador para a expressão e digite um valor para o atributo que se aplica às contas de usuário de destino. O valor pode ser parcial. Por exemplo, digite s* para procurar todos os registros em que o valor do atributo selecionado começar com a letra "s".

   Importante: Sempre digite critérios ao pesquisar para minimizar o tempo necessário para recuperar as entradas de um armazenamento de usuários externos.
6. Clique em Ir.

   Os nomes dos usuários globais que corresponderem aos critérios que você selecionou são exibidos no painel Usuários. Os nomes são exibidos no formato Sobrenome, Nome.

Exemplo: um indivíduo em dois Active Directories referenciados

Hipóteses:

- Antes de atualizar o CA Process Automation, o CA EEM fez referência a um diretório externo, um Microsoft Active Directory. A release do CA EEM era a r8.4.
- Posteriormente, mas ainda antes de atualizar o CA Process Automation, o CA EEM foi atualizado da release r8.4 para a r12.51. Os usuários do CA Process Automation, ou seja, usuários do AD referenciados que foram atribuídos a um grupo de aplicativos, mantiveram a atribuição de grupo após a atualização do CA EEM. Os usuários globais atribuídos ao grupo Criadores que eram proprietários de objetos de automação mantiveram a propriedade dos objetos.
- Durante a atualização para o CA Process Automation r4.2, o instalador selecionou a referência a vários ADs, um recurso com suporte no CA EEM r12.5.
- Agora, o administrador do CA EEM precisa atribuir um grupo de usuários de aplicativo para os usuários globais selecionados a partir dos ADs adicionais. O administrador também reatribui grupos de aplicativos para os usuários do CA Process Automation a partir do AD original.
- O administrador do CA EEM insere critérios de pesquisa para um usuário em um dos domínios do AD referenciados recentemente. Esse usuário está em dois domínios: no domínio existente e no novo. Embora, normalmente, cada usuário esteja em um domínio, é possível que os usuários estejam em mais de um domínio do AD. Quando isso acontece, as duas contas de usuário são tratadas como usuários diferentes, mesmo que elas se refiram à mesma pessoa.

O procedimento a seguir mostra como este exemplo seria exibido nos resultados da pesquisa do CA EEM e nos registros de usuário correspondentes.

Siga estas etapas:

1. Efetue logon no CA EEM como o administrador do CA EEM.
2. Clique em Gerenciar identidades. Digite os critérios de pesquisa para usuários globais. A pesquisa do exemplo é por todos os usuários do AD com o sobrenome Meier.

Search Users

Global Users

Attribute: Last Name

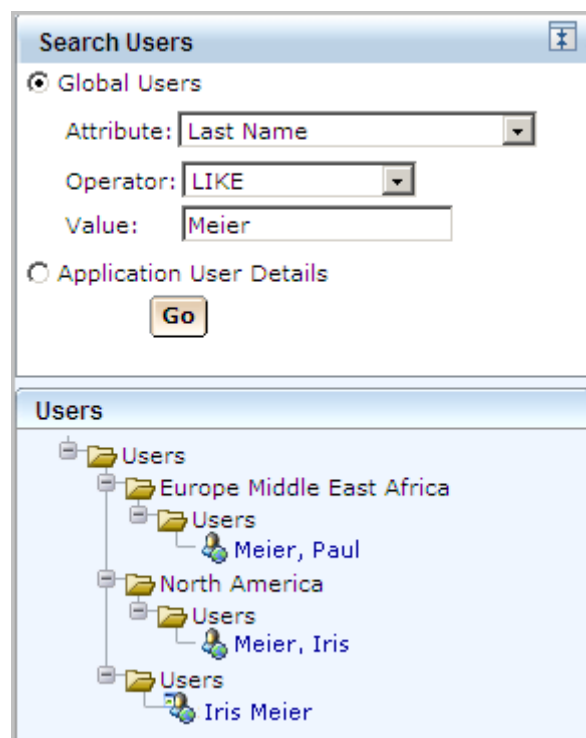
Operator: LIKE

Value: Meier

Application User Details

Go

Users

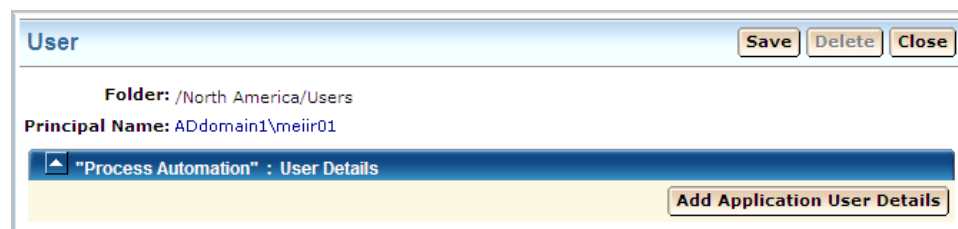
Users
Europe Middle East Africa
Users
Meier, Paul
North America
Users
Meier, Iris
Users
Iris Meier

2. Selecione um dos usuários globais exibidos, por exemplo, Meier, Iris. O painel Conta de usuário é exibido. Isto representa o registro do domínio do AD referenciado recentemente. Clique em Adicionar detalhes do usuário do aplicativo.

User Save Delete Close

Folder: /North America/Users

Principal Name: ADdomain1\meiir01

"Process Automation" : User Details

Add Application User Details

3. Selecione o grupo de usuários PAMAdmins para criar permissões de administrador para o CA Process Automation para esse usuário.

4. Selecione a outra entrada de usuário global nos resultados da pesquisa. Observe que essa exibe ADdomain2, não ADdomain1, e possui permissões de usuários de produção. Isto representa o registro de usuário existente.

User

Folder: /Users

Principal Name: ADdomain2\meiir01

"Process Automation" : User Details

Ren

Attributes

Application Group Membership

Available User Groups

Designers
PAMAdmins
PAMUsers
Production Users

Selected User Groups

Production Users

5. O usuário no domínio do AD referenciado originalmente poderá efetuar logon no CA Process Automation com o nome de usuário não qualificado, se esse domínio estiver definido como o domínio padrão. (Todos os usuários de outros domínios devem digitar seus respectivos nomes da entidade principal em Nome de usuário no momento do logon.) Portanto, neste exemplo, a entrada do nome de usuário não qualificado conecta o usuário com permissões de usuários de produção. Para obter a permissão do PAMAdmins, o usuário deverá digitar ADdomain1\meiir01 no campo Nome de usuário.

Sobre usuários globais

Todos os usuários definidos para o CA EEM são globais. Os tipos de usuário global podem ser os seguintes:

- Usuários para os quais são criadas contas de usuários globais, nas quais todos os detalhes são fornecidos, inclusive a atribuição de um grupo de aplicativos e a definição de uma senha.
- Usuários definidos no CA EEM para uso com outro produto da CA. Pesquise tais usuários globais e forneça acesso ao CA Process Automation atribuindo um grupo de aplicativos do CA Process Automation a cada usuário. Tais usuários globais efetuam logon no CA Process Automation com as credenciais definidas anteriormente no CA EEM.
- Usuários definidos em um armazenamento de usuários externo que você identificou ao instalar o CA EEM. Pesquise tais usuários globais e forneça acesso ao CA Process Automation atribuindo um grupo de aplicativos do CA Process Automation a cada usuário. Tais usuários globais efetuam logon no CA Process Automation com as credenciais definidas no armazenamento de usuários externo.

  Observação: os usuários digitam suas credenciais como o nome da entidade principal (*nome de domínio**nome de usuário*) e a senha ou o nome de usuário e a senha. O nome da entidade principal é *aceito* quando o CA EEM usa o Microsoft Active Directory como o armazenamento de usuários externo e vários domínios são referenciados durante a instalação. O nome da entidade principal é *obrigatório* quando o domínio do AD de origem para o usuário não é o domínio padrão.

Se você usar o armazenamento de usuários interno do CA EEM, você pode criar usuários globais e atribuir grupos de aplicativos. Se você fizer referência a um armazenamento de usuários externo, é possível recuperar os usuários globais e atribuir grupos de aplicativos.

Atribuir um grupo de aplicativos a um usuário global

Para conceder a um usuário o acesso com base em funções, atribua um grupo de aplicativos à respectiva conta de usuário global.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Pesquise identidades correspondentes aos critérios especificados (na página 64).
3. Em Usuários, selecione o nome do usuário de destino.

   A conta de usuário selecionada é aberta.
4. Clique em Adicionar detalhes do usuário do aplicativo.

   A caixa de diálogo Associação ao grupo de aplicativos é exibida.

5. Selecione o grupo apropriado em Grupos de usuários disponíveis e, em seguida, clique na seta para a direita (>) e mova-o para Grupos de usuários selecionados.
6. Clique em Salvar.

   Agora, o usuário global de destino pode efetuar logon no CA Process Automation. Após o processo de autenticação, o usuário poderá acessar a funcionalidade que o produto concede a todos os membros do grupo de aplicativos atribuído.

Sobre grupos de usuários dinâmicos

Um *grupo de usuários dinâmico* consiste em usuários globais que compartilham um ou mais atributos. Ele é criado por meio de uma diretiva especial de grupo de usuários dinâmico. O nome do recurso é o nome do grupo de usuários dinâmico e a associação baseia-se em filtros configurados em atributos de usuário e grupo.

É possível criar um grupo de usuários dinâmico que consiste em usuários, grupos de aplicativos, grupos globais ou grupos dinâmicos. Por exemplo, é possível criar um grupo de usuários dinâmico de grupos globais ou grupos de aplicativos com base no nome, na descrição ou na associação ao grupo. De maneira semelhante, pode-se criar um grupo de usuários dinâmico com funções diferentes com base em um atributo comum em seu perfil de usuário global. Por exemplo:

- Cargo
- Departamento ou escritório
- Cidade, estado ou país

O usuário EiamAdmin pode criar regras de diretivas de grupos dinâmicos de usuários.

Criar uma diretiva de grupo de usuários dinâmico

Você pode criar uma diretiva de grupo de usuários dinâmico.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique em Gerenciar diretivas de acesso e, em seguida, clique em Nova diretiva de grupo dinâmico à esquerda de Diretivas de grupo de usuários dinâmico.
3. Em Nome, digite um nome de grupo que identifique uma propriedade comum do grupo de usuários. Opcionalmente, digite uma descrição.
4. Selecione um tipo de diretiva. O padrão é Diretivas de acesso.

5. Selecione as identidades da seguinte maneira:

   a. Em Tipo, selecione um dos valores a seguir e, em seguida, clique em Procurar identidades.

      - Usuário
      - Grupo de aplicativos
      - Grupo global
      - Grupo dinâmico

   b. Em Atributo, Operador e Valor, digite a expressão que define os critérios da associação para o grupo e clique em Pesquisar.

      Exemplo:

      Selecione Usuário, digite **Cargo como gerente** e clique em Pesquisar. O processo retornará todos os usuários com o cargo Gerente.

   c. No resultado da pesquisa, selecione os usuários que deseja adicionar como integrantes desse grupo dinâmico. Para mover suas seleções para a lista de Identidades selecionadas, clique na seta para a direita (>).

6. Para Ações, selecione pertencer.

7. No campo Adicionar recurso, forneça o valor digitado no campo Nome e, em seguida, clique no botão Adicionar.

   O processo adicionará as identidades selecionadas ao grupo de usuários dinâmico que você criou.

8. (Opcional) Adicionar mais filtros.

9. Clique em Salvar.

   A diretiva que você criou é exibida quando você clica no link Diretivas de grupo de usuários dinâmico.

Capítulo 4: Administrar segurança avançada do CA EEM

Você pode usar o CA EEM para criar diretivas de acesso refinadas para atender aos mais rigorosos requisitos de segurança. É possível criar diretivas personalizadas, criar grupos que usam essas diretivas personalizadas e atribuir seus grupos personalizados para contas de usuário. Ou então, você pode atribuir usuários diretamente para as diretivas personalizadas. Você pode definir diretivas personalizadas para limitar o acesso a uma ou mais pastas especificadas com ou sem subpastas. Os níveis de acesso incluem exibir, navegar, editar, excluir e criar, onde as permissões são complementares. Você pode limitar o acesso de usuários a um ambiente especificado. Você também pode modificar o acesso definido para grupos padrão.

Personalização é necessária para estender o acesso padrão. Por exemplo, a personalização é usada para conceder acesso ao CA EEM aos administradores, criar acesso semelhante ao fornecido pela implementação LDAP e limitar o acesso aos servidores que contenham informações confidenciais ou processos de negócios críticos.

A seção Referência de permissões inclui os detalhes que oferecem suporte a todos os tipos de personalização.

Esta seção contém os seguintes tópicos:

Concedendo aos administradores acesso ao CA EEM

O CA EEM fornece segurança para o CA Process Automation. O CA EEM mantém as credenciais em contas de usuário que permitem que os usuários efetuem logon no CA Process Automation. O CA EEM autentica usuários no logon e permite efetuar logon se a ID de usuário e a senha forem encontradas em uma conta de usuário. As contas de usuário estão associadas a grupos. O CA EEM autoriza os usuários no logon com base em suas atribuições de grupo.

EiamAdmin é o nome de usuário predefinido do administrador do CA EEM. O administrador do CA EEM é a função que fornece aos usuários acesso ao CA Process Automation. Durante a instalação do CA Process Automation, é possível especificar uma senha para o usuário EiamAdmin. Apenas os usuários que souberem a senha do EiamAdmin poderão efetuar logon no CA EEM. Recomendamos que o conhecimento dessa senha seja restringido a apenas algumas pessoas confiáveis.

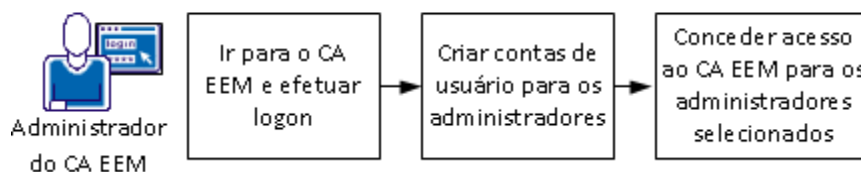
O usuário EiamAdmin pode definir uma diretiva que concede a administradores selecionados do CA Process Automation a capacidade de criar diretivas, contas de usuário e grupos personalizados. Esse acesso é suficiente, mas mais limitado que o do EiamAdmin. O processo é o seguinte:

Concedendo acesso de administrador ao CA EEM

Administrador do CA EEM

Ir para o CA EEM e efetuar logon

Criar contas de usuário para os administradores

Conceder acesso ao CA EEM para os administradores selecionados

1. Navegue até o CA EEM e efetue logon (na página 46).
2. Cria contas de usuário para administradores (na página 56).
3. Conceder aos administradores selecionados acesso ao CA EEM (na página 75).

Mais informações:

Conceder acesso ao CA EEM aos administradores selecionados (na página 75)

Conceder acesso ao CA EEM aos administradores selecionados

O acesso ao CA EEM é exigido para gerenciar contas de usuários, grupos e diretivas. Por padrão, é necessário saber a senha do EiamAdmin para efetuar logon no CA EEM com o aplicativo definido para o CA Process Automation. Em geral, o conhecimento dessa senha é altamente restrito, pois o usuário EiamAdmin tem controle total do CA EEM. No entanto, o usuário EiamAdmin pode conceder acesso de logon ao CA EEM a outros administradores e especificar os objetos que podem ser gerenciados por eles. O seguinte procedimento mostra como conceder aos administradores selecionados a capacidade de gerenciar contas de usuário, grupos e diretivas. Esse processo inclui definir um novo grupo, criar uma diretiva personalizada para o grupo e, em seguida, atribuir o grupo a contas de usuário.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Crie EEMAdmins, um grupo de administradores do CA EEM, cujos membros podem criar contas de usuário, grupos personalizados e diretivas personalizadas.
    a. Clique na guia Gerenciar identidades.
    b. Clique em Grupos.
    c. Clique em Novo grupo de aplicativos.
    d. Digite um nome para o grupo (por exemplo, EEMAdmins).
    e. (Opcional) Adicione uma descrição.
    f. Clique em Salvar.

    Observação: não selecione um grupo de aplicativos.

3. Crie uma diretiva que conceda a capacidade de criar contas de usuário, grupos personalizados e diretivas personalizadas. Atribua EEMAdmins como a identidade para essa diretiva.

    a. Clique na guia Gerenciar diretivas de acesso.

    b. Clique em Diretivas de escopo.

    c. Clique no link para Administrar objetos.

    d. Clique em Salvar como e digite um nome para esta diretiva (por exemplo, Administrar usuários e diretivas).

    e. Clique em OK.

    f. Selecione [Usuário] EiamAdmin e [Usuário] CERT-application-name na lista de Identidades selecionadas e clique em Excluir.

    g. Clique em Procurar identidades para grupo de tipos e, em seguida, clique em Pesquisar.

    h. Selecione o novo grupo (EEMAdmins) e clique na seta para a direita para mover o grupo de usuários para Identidades selecionadas.

    i. Selecione e exclua todos os recursos, *exceto* ApplicationInstance, Policy, User, UserGroup, GlobalUser, GlobalUserGroup e Folder.

    j. Verifique se as opções ler e gravar estão selecionadas.

    k. Clique em Salvar.

    Sua diretiva se parece com o seguinte exemplo:

Diretivas de escopo

Nome/Descrição	Nome da classe do recurso	Opções	Identidades	Ações	Recursos
Administrater Users and Policies System Default: administrative access for the installer and the application instance certificate	SafeObject	Concessão explícita	ug:EEMAdmins	read write	ApplicationInstance Policy User UserGroup GlobalUser GlobalUserGroup Folder

4. Adicione o grupo EEMAdmins às contas de usuário dos administradores selecionados:
    a. Clique na guia Gerenciar identidades.
    b. Clique em Detalhes do usuário do aplicativo para Pesquisar usuários.
    c. Selecione Associação ao grupo como atributo, LIKE como operador e PAMAdmins como valor.
    d. Clique em Ir.

        Os administradores do CA Process Automation são listados.
    e. Clique no nome de um administrador.

        A conta de usuário do administrador selecionado é exibida. EEMAdmins é exibido como um grupo de usuários disponível.
    f. Clique na seta para a direita para mover EEMAdmins para Grupos de usuários selecionados.
    g. Clique em Salvar.
5. Repita a Etapa 4 para cada administrador ao qual você deseja conceder direitos do CA EEM.

Personalizando o acesso do usuário com diretivas do CA EEM

Você pode personalizar o acesso do usuário às guias e paletas do CA Process Automation e o acesso a diferentes objetos de automação. Para estender as alterações para todos os usuários no grupo padrão, você pode alterar as diretivas padrão.

Você pode restringir o acesso do usuário a pastas especificadas. Por exemplo, você pode criar uma pasta para cada criador e restringir o acesso do criador a própria pasta e a pastas criadas para uso comum.

Você pode restringir o acesso a um ambiente especificado para os usuários especificados. Por exemplo, você pode restringir o acesso ao ambiente para os membros do grupo Usuários de produção, de forma que eles possam acessar apenas o ambiente de produção. Desse modo, eles não podem acessar o ambiente de criação.

Você pode restringir o acesso a touchpoints mapeados para os servidores que contenham informações confidenciais ou executem uma função de negócios crítica com as diretivas de segurança do touchpoint.

Caches de controle de atualizações do CA EEM

O CA Process Automation não reflete imediatamente as alterações quando diretivas, grupos de usuários e contas de usuário são modificadas no CA EEM. O CA Process Automation nem sempre consulta diretamente o CA EEM para as consultas de autorização. O CA EEM não envia alterações específicas ao CA Process Automation à medida que elas ocorrem. Em vez disso, o CA Process Automation depende dos caches a seguir:

- Um cache no CA EEM de alterações em diretivas, grupos de usuários e contas de usuário que o CA EEM envia ao CA Process Automation.

  Uma configuração de segurança na guia Configuração controla a taxa de atualização do cache. É possível atualizar a configuração em nível de domínio ou para um ambiente selecionado.

- Um cache secundário no CA Process Automation de resultados da consulta que o CA EEM retorna ao CA Process Automation.

  Quando a função de segurança valida as permissões de usuário, verifica primeiro a duração do cache secundário.

  - Se a duração do cache for igual ou menor que o valor configurado, a função de segurança usará os dados de permissão no cache.
  - Se a duração do cache for maior que o valor configurado, a função de segurança enviará uma solicitação para o CA EEM. A função de segurança atualiza o cache secundário com os resultados da consulta e redefine a duração do cache para 0 segundo.

Ao testar as diretivas personalizadas com um usuário de teste, é possível exibir os resultados assim que o CA EEM envia as alterações para o CA Process Automation. Para atualizar o CA Process Automation com mais frequência, reduza o intervalo de atualização. Para otimizar o desempenho do produto quando você concluir o teste, aumente o intervalo de atualização do cache.

Quando usar o procedimento a seguir para alterar a taxa de atualização do cache no CA EEM, considere o uso de uma taxa de atualização rápida apenas no ambiente de criação. Como opção, altere a duração máxima do cache secundário no servidor que hospeda o orquestrador de destino para teste.

Siga estas etapas:

1. Altere a frequência com que o CA Process Automation recebe atualizações do CA EEM. Defina o intervalo padrão em nível de domínio.
    a. Clique na guia Configuração.

       A paleta Navegador de configuração é aberta com Domínio selecionado. A guia Segurança é exibida.

    b. Clique em Bloquear.

    c. Edite a configuração de Intervalo entre atualizações do cache do CA EEM (em segundos), conforme necessário, com base na frequência com que o CA EEM será atualizado.

       - Ao testar o impacto das alterações do CA EEM, defina o intervalo de atualização como **60** segundos.
       - Quando concluir o teste, defina o intervalo de atualização para **1.800** segundos (padrão).

    d. Clique em Salvar.

    e. Selecione Domínio e clique em Desbloquear.

    f. Reinicie o Orquestrador de domínio.

       - Interrompa o orquestrador (na página 193).
       - Inicie o orquestrador (na página 194).

2. Altere a frequência com que o CA EEM envia alterações de autorização para o CA Process Automation em um ambiente selecionado.
   a. Clique na guia Configuração e expanda Domínio, na paleta Navegador de configuração.
   b. Selecione o ambiente de destino e clique em Bloquear.
   c. Na guia Segurança, edite a configuração de Intervalo entre atualizações do cache do CA EEM (em segundos), conforme necessário, se você estiver executando os testes de autorização de usuário.
      - Enquanto estiver testando as personalizações, defina o intervalo de atualização como **60** segundos.
      - Quando concluir o teste, defina o intervalo de atualização para **1.800** segundos (padrão).
   d. Clique em Salvar.
   e. Selecione o ambiente e clique em Desbloquear.
   f. Reinicie os orquestradores no ambiente atualizado.
      - Interrompa o orquestrador (na página 193).
      - Inicie o orquestrador (na página 194).
3. Altere a duração máxima (em segundos) do cache secundário que contém permissões de usuário.

   Observação: normalmente não é necessário alterar esse parâmetro interno.
   a. Efetue logon no servidor em que o orquestrador de destino está configurado.
   b. Vá até a seguinte pasta ou diretório:

      dir_instalação/server/c2o/.config/
   c. Abra o arquivo OasisConfig.properties
   d. Adicione o seguinte parâmetro, se ele não existir:

      `eem.cache.timeout`
   e. Atribua um valor (em segundos).

      A definição desse parâmetro como 0 desativa esse cache para que o CA Process Automation solicite permissões de usuário do CA EEM quando necessário. O produto usa o valor padrão (30) quando esse parâmetro não está presente no arquivo OasisConfig.properties.

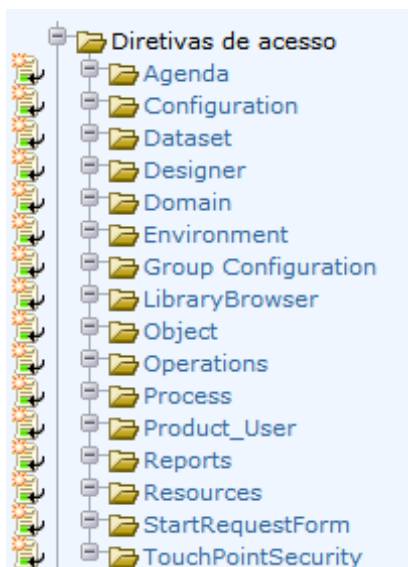
      `eem.cache.timeout=30`
   f. Salve o arquivo.
   g. Reinicie o serviço do orquestrador.
      - Interrompa o orquestrador (na página 193).
      - Inicie o orquestrador (na página 194).

Mais informações:

Configurar as definições de segurança do CA EEM para o domínio (na página 140)

Classes de recursos padrão e diretivas personalizadas

As classes de recursos do CA Process Automation estão listadas nas políticas de acesso em CA EEM. Você pode criar uma diretiva personalizada original para qualquer classe de recursos ou baseá-la em uma diretiva predefinida.

Diretivas de acesso
- Agenda
- Configuration
- Dataset
- Designer
- Domain
- Environment
- Group Configuration
- LibraryBrowser
- Object
- Operations
- Process
- Product_User
- Reports
- Resources
- StartRequestForm
- TouchPointSecurity

A maioria das classes de recursos do CA EEM inclui diretivas predefinidas.

Você pode usar a opção Salvar como para salvar as diretivas de acesso predefinidas com um novo nome e, em seguida, personalizá-las, conforme necessário. Criar uma diretiva personalizada com base em uma diretiva predefinida irá ajudá-lo a obter os seguintes resultados:

- Fornecer ao grupo atribuído uma permissão que a diretiva predefinida não concede. Por exemplo, a diretiva personalizada pode conceder ao grupo Criadores acesso à paleta Instalação na guia Configuração, de forma que eles possam instalar os agentes.
- Remover uma permissão ou acesso que uma diretiva predefinida concede. Por exemplo, a diretiva personalizada pode remover os direitos de acesso do grupo PAMUsers à guia Relatórios.
- Substituir um grupo padrão (por exemplo, PAMAdmins) por grupos que melhor reflitam as funções do produto que o seu site define. Por exemplo, é possível ter três níveis de administrador, em vez de um. Atribuir PAMAdmins para o administrador de domínio e criar diferentes grupos de administradores que administram o conteúdo e executam configurações para cada ambiente.

  Observação: para obter mais informações sobre como criar direitos de acesso separados para administradores de conteúdo e administradores de configuração, consulte o tópico Criar contas de usuário com funções personalizadas do AD (na página 114).
- Adicionar um ou mais filtros para um acesso refinado. Por exemplo, você pode especificar ENVIRONMENT igual a um nome de ambiente como um filtro. Muitas vezes, o filtro de ambiente é usado nas diretivas Segurança do touchpoint definidas pelo usuário.

Considere os objetos do processo e do formulário de solicitação inicial em termos de chamadas SOAP de nível de acesso por meio dos serviços web. Ao criar uma diretiva com a classe de recurso de processo, você concede os direitos Process Start (Iniciar) ou Process_Control (Controlar) aos usuários ou grupos especificados. Se o usuário que chamar o método Executar processo tiver a permissão Iniciar ou a permissão Controlar, o método será executado com êxito. Ao criar uma diretiva com a classe de recurso de formulário de solicitação inicial, você concede a usuários ou grupos especificados as permissões StartRequestForm_Start (Iniciar) ou StartRequestForm_Dequeue (Retirar da fila). Se o usuário que executar o método Executar formulário de solicitação inicial tiver a permissão Iniciar ou a permissão Retirar da fila, o método será executado com êxito. Se o usuário que executar o método não tiver direitos de execução no objeto de destino, o método falhará. O conjunto de dados do operador SOAP registra as mensagens de erro do método.

É possível criar uma diretiva personalizada do CA EEM que concede ou nega o acesso de grupos especificados a qualquer objeto de automação especificado. Por exemplo:

- Limitar o acesso a um ambiente especificado com as diretivas Agenda, Conjunto de dados, Sistema, Processo, Recursos, Formulário de solicitação inicial e Segurança do touchpoint. Adicionar um filtro em que o Ambiente é o atributo nomeado e seu nome de ambiente é o valor. O Operador CADEIA DE CARACTERES É IGUAL a = =. No seguinte exemplo de filtro, Teste é o nome do ambiente:

Tipo/valor à esquerda	Operador	Tipo/valor à direita
atributo nomeado	STRING	valor
ENVIRONMENT	EQUAL ==	Test

- Limitar o acesso a uma pasta ou objeto especificados com a diretiva Objeto. Adicionar um recurso, como /*nome_da_pasta* ou /*nome_da_pasta*/*nome_do_objeto*. No exemplo a seguir, /folder_name representa o nome da pasta em que o objeto de automação reside.

Recursos	Ações
Adicionar recurso:	Object_List Object_Read Object_Edit Object_Delete Object_Admin [Todas as ações]
/folder_name	☑ ☐ ☐ ☐ ☐ ☐

Você também pode criar uma diretiva personalizada para a classe de recurso do objeto. Diretivas no objeto fornecem um filtro para especificar o tipo de objeto para o qual a diretiva se aplica. Adicionar um filtro em que o atributo nomeado é o tipo de objeto e o valor é um tipo de objeto. O Operador CADEIA DE CARACTERES É IGUAL a = =. No seguinte exemplo de filtro, Recursos é o nome do tipo de objeto:

Tipo/valor à esquerda	Operador	Tipo/valor à direita
atributo nomeado	STRING	valor
OBJECT_TYPE	EQUAL ==	Package

Outros valores válidos incluem:

- As classes de recurso:
  - Agenda, a classe de recurso para programação.
  - Conjunto de dados
  - Processo
  - Recursos
  - Formulário de solicitação inicial
- Calendário
- Ícone personalizado
- Operador personalizado
- Pasta
- Formulário de solicitação de interação
- Exibição de processos

Como personalizar o acesso a um grupo padrão

Você pode personalizar o acesso padrão das seguintes maneiras:

- Adicionar uma ação a um grupo padrão.
- Revogar uma ação de um grupo padrão.

Todas as alterações feitas nas atribuições de um grupo padrão afetarão todos os usuários que estiverem atribuídos a esse grupo.

O processo de personalizar o acesso a um grupo padrão é o seguinte:

1. Verificar permissões para grupos padrão (na página 48).
2. Identificar a permissão necessária em seu site que um grupo padrão não possui.
3. Determinar a ação e a diretiva que controla esse acesso.
   - Se a permissão for para acessar uma guia ou paleta, consulte o tópico Permissões por guia (na página 100).
   - Se a permissão for em um objeto de automação, consulte o tópico Permissões em objetos de automação (na página 106).
4. Criar uma diretiva com base em uma diretiva existente (na página 85), onde a diretiva existente é uma diretiva padrão predefinida.
5. Conceder ou revogar uma ação para um grupo padrão (na página 85).

Criar uma diretiva personalizada com base em uma diretiva existente

É possível criar uma diretiva personalizada com base em uma diretiva padrão ou com base em outra diretiva personalizada.

O CA Process Automation fornece uma diretiva para quase todas as classes de recursos. Você pode modificar as diretivas padrão diretamente, pois elas são editáveis. No entanto, não há nenhum modo fácil para reverter para o estado original. Você pode instituir uma prática que preserva as diretivas predefinidas para que você possa comparar uma revisão com o original ou reverter para ele.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique em Manage Access Policies.
3. Clique no nome da diretiva de acesso a ser modificada.
4. Clique no link da diretiva na tabela de diretivas.
5. Clique em Salvar como e digite um nome de diretiva personalizada.
6. Clique em Salvar.
7. Se a diretiva personalizada for substituir uma diretiva predefinida, abra a diretiva predefinida e clique em Desativar. Em seguida, clique em Salvar.

Observação: a diretiva personalizada está pronta para personalização.

Conceder ou revogar uma ação para um grupo padrão

Você pode conceder uma nova ação para um grupo padrão. É possível também revogar uma ação predefinida de um grupo padrão.

Siga estas etapas:

1. Abra a diretiva personalizada que você criou para essa finalidade.
2. Na linha Criadores de Identidades selecionadas, marque ou desmarque a ação que você identificou.

   Observação: consulte o tópico Exemplo: conceder aos criadores a capacidade de executar instalações (na página 86).
3. Clique em Salvar.

   Sua diretiva personalizada entrará em vigor na próxima vez em que o CA EEM enviar atualizações para o CA Process Automation.

Exemplo: conceder aos criadores a capacidade de executar instalações

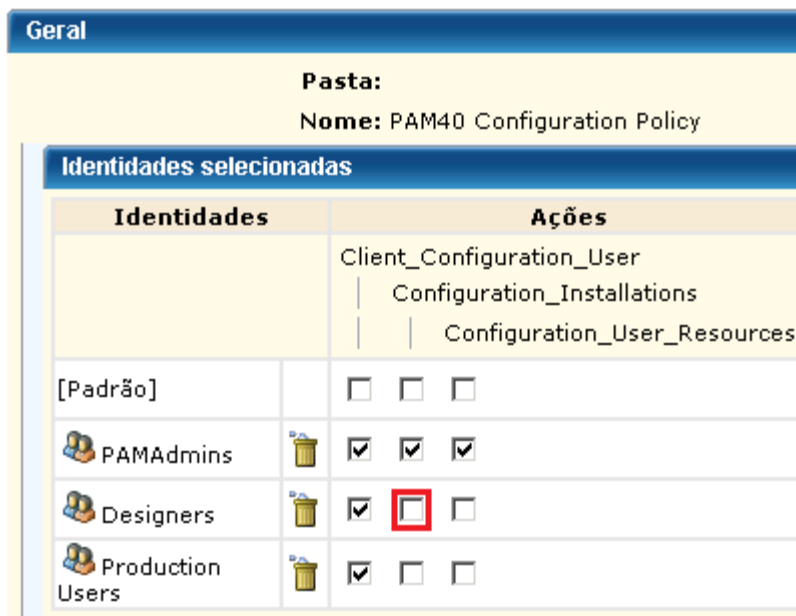
Por padrão, os criadores não tem acesso à paleta Instalação na guia Configuração. É possível adicionar a capacidade de instalar agentes aos usuários do grupo Criadores. Verifique Configuration_Installations (Instalações) de Criadores na diretiva de configuração PAM40.

Geral

Pasta:

Nome: PAM40 Configuration Policy

Identidades selecionadas

Identidades		Ações: Client_Configuration_User	Configuration_Installations	Configuration_User_Resources
[Padrão]		☐	☐	☐
PAMAdmins		☑	☑	☑
Designers		☑	☐	☐
Production Users		☑	☐	☐

Exemplo: Conceder aos criadores a capacidade de configurar grupos para operadores personalizados

Por padrão, os criadores não podem executar as seguintes ações em grupos para operadores personalizados:

- Bloquear a configuração de grupo de um operador personalizado
- Definir um grupo com variáveis apropriadas para um conjunto de operadores personalizados
- Desbloquear a configuração do grupo publicando o grupo

Grupos de operadores personalizados publicados são exibidos na guia Módulos no Navegador de configuração.

É possível conceder aos criadores de conteúdo permissão para criar e publicar grupos de operadores personalizados.

Siga estas etapas:

1. Efetue logon no CA EEM.
2. Clique em Manage Access Policies.

3. Abra a diretiva Configuração do grupo.

   a. Clique em Configuração do grupo.

   b. Clique no link da diretiva Configuração do grupo PAM40.

4. Adicione o grupo de aplicativos Criadores à lista Identidades selecionadas.

   a. Selecione Grupo de aplicativos na lista suspensa Tipo.

   b. Clique em Pesquisar identidades.

   c. Aceite as entradas padrão dos seguintes campos e clique em Pesquisar:

      - **Atributo:** Nome
      - **Operador:** LIKE
      - **Valor:** este campo fica em branco por padrão.

   d. Selecione Criadores e clique na seta para baixo:

5. Selecione a ação Group_Config_Admin para grupo Criadores.

6. Clique em Salvar.

Como restringir o acesso por ambiente

Os grupos padrão Criador e Usuário de produção são projetados para o caso típico em que há dois ambientes:

- Ambiente de criação (ambiente padrão)
- Ambiente de produção (ambiente definido pelo usuário)

Integrantes do grupo Criador criam os processos de negócios automatizados no ambiente de criação. Os criadores criam processos, formulários de solicitação de interação e conjuntos de dados, por exemplo.

Os integrantes do grupo Usuário de produção usam os processos, formulários e conjuntos de dados criados. Por exemplo, os usuários de produção iniciam processos, inspecionam conjuntos de dados e respondem a solicitações de interação.

É possível salvar as diretivas a seguir como diretivas personalizadas para restringir o grupo Criadores para o ambiente de criação e os usuários de produção para o ambiente de produção.

- Agenda
- Conjunto de dados
- Processo
- Recursos
- Formulário de solicitação inicial

Exemplo: filtro de ambiente

É possível limitar o acesso a programações por ambiente. Por exemplo, você pode usar o ambiente padrão para criar e adicionar um ambiente de produção para usar os processos e objetos relacionados que foram passados para a produção.

O exemplo de filtro a seguir para programações restringe os integrantes do grupo Criadores para o ambiente padrão. Isso restringe os integrantes do grupo Usuários de produção para o ambiente de produção.

Nome/Descrição	Nome da classe do recurso	Filtros
Custom Schedule Policy with Environment Restrictions Restrict Schedule automation object for Designer group to Default Environment and Production User group to Production Environment	Agenda	ONDE ((ug:Name == val:Designers E req:action {} val:Agenda_Control E name:ENVIRONMENT == val:Default Environment) OU (ug:Name == val:Production Users E req:action {} val:Control E name:ENVIRONMENT == val:Production Environment))

Você pode personalizar as diretivas com base nas diretivas padrão com filtros semelhantes a seguir:

- Diretiva Conjunto de dados PAM40
- Diretiva Processo PAM40
- Diretiva Formulário de solicitação inicial PAM40
- Diretiva Recursos PAM40

Abra a diretiva padrão. Salve-a como uma diretiva personalizada. Altere o tipo para Diretiva de acesso. Em seguida, adicione o filtro.

Como personalizar o acesso com um grupo personalizado

O procedimento básico para personalizar o acesso com um grupo personalizado é o seguinte:

1. Criar um grupo personalizado (na página 89).
2. Adicionar o grupo personalizado a uma diretiva padrão (na página 91).

   Aqui, você concede permissões para as ações especificadas ao grupo personalizado.
3. Atribuir o grupo personalizado para contas de usuário (na página 92).

   Você pode atribuir mais de um grupo para uma conta de usuário para estender as permissões desse usuário.

Observação: para encontrar exemplos desse procedimento, consulte o tópico Como realizar a transição de funções utilizadas no Active Directory para o CA EEM (na página 114).

Criar um grupo personalizado

Você pode criar um grupo de usuários do aplicativo personalizado no CA EEM. Para conceder direitos a esse grupo, adicione-o a diretivas e selecione as ações apropriadas. Por fim, atribua o grupo a contas de usuários individuais.

Observação: as diretivas às quais um grupo personalizado deve ser adicionado variam se o grupo tiver como base um grupo existente.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.
3. Clique em Grupos.
4. No painel Grupos, clique no botão Novo grupo de aplicativos ao lado de Grupos de aplicativos para criar um grupo personalizado.

5. Digite um nome para o grupo no campo Nome.
6. (Opcional) Insira uma descrição para o grupo.
7. (Opcional) No grupo de seleção Associação ao grupo de aplicativos, selecione PAMUsers para incluir permissões para acesso básico. Nesse caso, você pode limitar as permissões concedidas a este grupo personalizado. Não é necessário conceder permissões que são concedidas ao grupo PAMUsers.

   Observação: se você deixar a área Grupos de usuários selecionados em branco, o grupo personalizado deverá incluir as permissões de acesso básico.
8. Clique em Salvar.

   O produto exibirá o novo grupo como um grupo de usuários do aplicativo quando você definir novos usuários.
9. (Opcional) Selecione Mostrar grupos de aplicativos em Pesquisar grupos e, em seguida, clique em Ir.

   O produto exibe o novo grupo com outros grupos (incluindo os grupos padrão).
10. Clique em Fechar.

Mais informações:

Adicionar um grupo personalizado para uma diretiva padrão (na página 91)

Adicionar um grupo personalizado para uma diretiva padrão

Uma maneira simples para personalizar os privilégios de acesso é criar grupos personalizados e adicionar os grupos para as diretivas padrão selecionadas. Com essa abordagem, não é possível criar políticas personalizadas. Identifique as ações ou permissões nas diretivas padrão que indivíduos que atribuídos ao grupo personalizado necessário.

Siga estas etapas:

1. Navegue até o CA EEM e efetue logon (na página 46).
2. Crie um grupo personalizado para usuários que executarão o mesmo conjunto de tarefas no CA Process Automation.
   a. Clique na guia Gerenciar identidades.
   b. Clique em grupos.
   c. Clique em Novo grupo de aplicativos.
   d. Digite o nome do grupo.
   e. Não adicione uma associação ao grupo de aplicativos.
   f. Clique em Salvar.
3. Abra a diretiva padrão que contém a ação que deseja conceder.
   a. Clique na guia Manage Access Policies.
   b. Clique no link para a classe de recurso apropriada em diretivas de acesso.
   c. Clique no link na tabela de diretivas para a diretiva ser atualizada.

      A diretiva selecionada é aberta.
4. Conceda a permissão selecionada ao grupo personalizado.
   a. Em Inserir/Pesquisar identidades, selecione o grupo de aplicativos na lista suspensa de tipo e clique em pesquisar.
   b. Selecione o grupo personalizado na lista e clique na seta para baixo.
   c. O grupo personalizado é exibido na lista de identidades selecionadas.
   d. Selecione a caixa de seleção para cada ação a ser concedida.
   e. Clique em Salvar.

   O grupo personalizado é adicionado à diretiva de usuário selecionada.

Atribuir um grupo personalizado para contas de usuário

Você pode atribuir um grupo personalizado (função) para uma conta de usuário durante o processo de criação dessa conta de usuário. Ou, você pode editar uma conta de usuário existente para adicionar o novo grupo de usuários do aplicativo.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.
3. Crie ou acesse a conta de usuário de destino.
   - Clique em Novo usuário para adicionar uma conta de usuário.
   - Use Procurar usuários para recuperar uma conta de usuário existente.
4. Se criar uma nova conta, digite a ID da conta de usuário no campo Nome, digite os detalhes sobre o usuário em Detalhes do usuário global, digite uma senha temporária e selecione Alterar senha no próximo login.
5. Clique em Adicionar detalhes do usuário do aplicativo.
6. Selecione o grupo personalizado em Grupos de usuários disponíveis e clique em > para movê-lo a Grupos de usuários selecionados.
7. Clique em Salvar e, em seguida, clique em Fechar.
8. Repita para cada usuário que receberá as permissões para o grupo personalizado.
9. Clique em Logoff.

Como personalizar o acesso para um usuário especificado

Você pode restringir os objetos que um usuário especificado do CA Process Automation pode exibir e as ações que ele pode executar. É possível criar regras do CA EEM, de forma que um usuário só possa ver e usar uma instância de objeto de automação ou um objeto de automação. Esse tipo de acesso é possível somente quando os criadores de conteúdo trabalham com objetos de biblioteca em pastas de trabalho. Nesse caso, as versões da release de objetos são copiadas para uma pasta específica da release para exportação como pacote de conteúdo.

Siga estas etapas:

1. Configure pastas específicas para criadores (na página 94).
2. Crie uma conta de usuário sem atribuição de grupo (na página 94).
3. Adicione o usuário às diretivas padrão selecionadas (na página 96).
4. Crie uma diretiva Objeto personalizada com as permissões de caminho (na página 98).
5. Crie uma diretiva personalizada para um tipo de objeto especificado (na página 99).

Observação: efetue logon no CA Process Automation como o usuário especificado e verifique se o acesso está correto.

Configurar pastas específicas para criadores

É possível criar a estrutura de pastas a seu critério. Para obter um acesso refinado, crie a estrutura para que você possa especificar um caminho para os objetos de um determinado tipo na diretiva desse objeto de automação. Para restringir um usuário (ou grupo) para tipos de objeto específicos ou para tipos de objeto específicos em determinados projetos, configure uma estrutura de pastas que permita essa restrição. Por exemplo, configure uma pasta WIP (Work In Progress - Trabalho em Andamento) com uma pasta para cada criador.

WIP/designer1

Cada criador tem uma pasta de trabalho separada. Cada pasta de criador contém um conjunto de pastas, uma para cada tipo de objeto de automação no qual o desenvolvedor trabalha. Uma pasta de conjunto de dados pode conter conjuntos de dados de vários projetos desenvolvidos por um único criador.

/project1/releaseVersion1

Cada projeto tem uma determinada pasta, com uma subpasta para cada versão da release. Quando uma versão da release de um processo estiver pronta para a transição para a produção, copie os objetos das pastas de trabalho para a pasta da versão da release. A pasta da versão da release é a pasta que o produto exporta como pacote de conteúdo.

Siga estas etapas:

1. Navegue para o CA Process Automation e efetue logon (na página 18).
2. Clique na guia Biblioteca.
3. Selecione a pasta raiz, clique em Novo e, em seguida, selecione Pasta.
4. Digite um nome curto para a nova pasta.
5. Repita essas etapas, conforme apropriado, para criar a estrutura de pastas necessária.

Criar uma conta de usuário sem atribuição de grupo

É possível criar uma conta de usuário sem atribuição de grupo. Esta é uma parte do processo de criação de acesso refinado, onde você restringe o usuário para criar e testar os objetos de um tipo específico.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.

3. Clique no ícone ao lado de Usuários na paleta Usuários.

   A página Novo usuário é exibida.

4. Digite a ID de usuário para atribuir à conta de usuário no campo Nome.

   Esse nome é o nome que o usuário digita no campo Nome de usuário no momento do logon.

5. Insira os detalhes do usuário global.

   a. Digite o nome nos campos Nome e Sobrenome.

      A barra de títulos exibe esses valores quando o usuário efetua logon no CA Process Automation.

   b. Preencha os outros campos na área Geral conforme apropriado.

6. (Opcional) Preencha o campo Associação de grupo global se você usar o CA Process Automation com outro produto da CA Technologies que usa esse CA EEM.

7. Digite e confirme uma senha para associar à conta na área Autenticação.

   Forneça aos usuários a senha temporária que você configurar para que eles possam alterar suas próprias senhas.

8. (Opcional) Preencha os campos restantes na página Novo usuário.

9. Clique em Salvar e, em seguida, clique em Fechar.

10. Clique em Logoff.

Adicionar o usuário às diretivas padrão selecionadas

Você pode conceder permissões do CA Process Automation para uma identidade de usuário usando ambas ou uma das seguintes maneiras:

- Atribuir um grupo de usuários à conta de usuário.
- Adicionar a conta de usuário às diretivas selecionadas. Em cada diretiva, atribuir ações selecionadas para a identidade do usuário.

Se estiver trabalhando com a diretiva personalizada e funções de usuário refinadas, recomendamos que você conceda acesso básico, atribuindo o grupo PAMUsers à conta de usuário e, em seguida, ampliando esse acesso com atribuições de ação de diretivas.

Se preferir conceder o acesso apenas com as diretivas, comece fornecendo acesso básico. Adicione o nome da conta de usuário às seguintes diretivas e ações:

- Diretiva de logon de usuário PAM40: Console-Login (Usuário)
- Diretiva de ambiente PAM40: Environment_Library_User (Usuário)
- Diretiva de navegador da biblioteca PAM40: LibraryBrowser_User (Usuário do navegador da biblioteca)

É possível conceder acesso refinado para a guia Operações. Você pode limitar o acesso de usuários a ações específicas em tipos de objeto específicos.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar diretivas de acesso.
3. Adicione o usuário à diretiva de logon de usuário PAM40.
    a. Clique no link Usuário de produto em Diretivas de acesso.
    b. Clique no link Diretiva de logon de usuário PAM40 na Tabela de diretivas.
    c. Defina Tipo como **Usuário** e clique em Procurar identidades.
    d. Clique em Pesquisar.
    e. Selecione o identificador de usuário na lista exibida e clique na seta para baixo.
    f. Selecione Console-Login (Usuário) para o usuário adicionado.
    g. Clique em Salvar e em Fechar.

4. Adicione o usuário à diretiva de ambiente PAM40.
   a. Clique no link Ambiente em Diretivas de acesso.
   b. Clique no link Diretiva de ambiente PAM40 na Tabela de diretivas.
   c. Defina Tipo como **Usuário** e clique em Procurar identidades.
   d. Clique em Pesquisar.
   e. Selecione o identificador de usuário na lista exibida e clique na seta para baixo.
   f. Selecione Environment_Library_User (Usuário) para o usuário adicionado.
   g. Clique em Salvar e em Fechar.
5. Adicione o usuário à diretiva de navegador da biblioteca PAM40.
   a. Clique no link Navegador da biblioteca em Diretivas de acesso.
   b. Clique no link Diretiva de navegador da biblioteca PAM40 na Tabela de diretivas.
   c. Defina Tipo como **Usuário** e clique em Procurar identidades.
   d. Clique em Pesquisar.
   e. Selecione o identificador de usuário na lista exibida e clique na seta para baixo.
   f. Selecione LibraryBrowser_User (Usuário do navegador da biblioteca) para o usuário adicionado.
   g. Clique em Salvar e em Fechar.
6. Conceda o acesso de usuário a dois objetos na guia Operações. Adicione o usuário à diretiva de operações PAM40 e especifique apenas duas ações.
   a. Clique no link Operações em Diretivas de acesso.
   b. Clique no link Diretiva de Operações PAM40 na Tabela de diretivas.
   c. Defina Tipo como **Usuário** e clique em Procurar identidades.
   d. Clique em Pesquisar.
   e. Selecione o identificador de usuário na lista exibida e clique na seta para baixo.
   f. Selecione Operations_Datasets (Conjuntos de dados) para o usuário adicionado.
   g. Selecione Operations_Resources (Recursos) para o usuário adicionado.
   h. Clique em Salvar e em Fechar.

Criar uma diretiva Objeto personalizada com as permissões de caminho

Criar uma diretiva de acesso Objeto personalizada com a diretiva de acesso Objeto. O número de entradas depende da profundidade do caminho. Digite uma linha para cada nível do caminho, começando com a pasta raiz (/).

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Manage Access Policies.
3. Crie uma diretiva Objeto personalizada para restringir um usuário especificado para um caminho especificado na biblioteca.
    a. Clique no link Nova diretiva de acesso para Objeto em Diretivas de acesso.
    b. Digite um nome.
    c. Selecione a lista de controle de acesso para Tipo e clique em OK para verificar a mensagem.
    d. Clique em Procurar identidades com o tipo definido para Usuário.
    e. Clique em Pesquisar. Selecione o identificador de usuário na lista exibida e clique na seta para a direita.
    f. Digite uma barra (/) no campo Adicionar recurso e clique em Adicionar.
    g. No mesmo campo, digite / seguido pelo nome da pasta que contém os objetos para os quais o usuário é restrito. Clique em Adicionar.
    h. Selecione Object_List (Lista) para a pasta raiz (/).
    i. Selecione Object_List (Lista) para o caminho /*folder*. Repita essa etapa se houver um caminho /*folder*/*subfolder*.

       Observação: é possível digitar /folder/subfolder* e selecionar "Tratar como expressão regular" para incluir todas as pastas subordinadas na subpasta especificada.
    j. Clique em Salvar. Clique em Fechar.

Criar uma diretiva personalizada para um tipo de objeto especificado

Crie uma diretiva para o tipo de objeto para o qual a restrição se aplica. Em seguida, especifique as ações a permitir no tipo de objeto selecionado. Escolha entre os seguintes tipos de diretivas:

- Agenda
- Conjunto de dados
- Processo
- Recursos
- Formulário de solicitação inicial

Observação: para obter detalhes sobre permissões, consulte a seção Referência de permissões (na página 100).

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Manage Access Policies.
3. Crie uma diretiva personalizada para o tipo de objeto que você deseja restringir.
   a. Clique no link Nova diretiva de acesso para um dos seguintes tipos de recursos: Agenda, Conjunto de dados, Processo, Recursos, Formulário de solicitação inicial.
   b. Digite um nome.
   c. Selecione a lista de controle de acesso para Tipo e clique em OK para verificar a mensagem.
   d. Clique em Procurar identidades com o tipo definido para Usuário.
   e. Clique em Pesquisar. Selecione o identificador de usuário na lista exibida e clique na seta para a direita.
   f. No campo Adicionar recurso, digite o caminho completo que contém o tipo de objeto que você selecionou. Clique em Adicionar.
   g. No mesmo campo, digite uma barra (/) e, em seguida, digite o nome da pasta que contém os objetos para os quais o usuário é restrito. Clique em Adicionar.
   h. Selecione a permissão a ser concedida.
      - Agenda: Agenda_Control (Controlar). Agenda refere-se a programações.
      - Conjunto de dados: Dataset_Inspect (Inspecionar), Dataset_Modify (Modificar).
      - Processo: Process_Control (Controlar), Process_Monitor (Monitorar), Process_Start (Iniciar).
      - Recursos: Resources_Control

i. Clique em Salvar. Clique em Fechar.

4. (Opcional) Adicione um filtro para limitar por ambiente.
5. Repita esse procedimento para objetos dependentes. Considere, por exemplo, Conjuntos de dados. Conjuntos de dados são significativos apenas no contexto de um outro tipo de objeto. Se você selecionar Conjuntos de dados, crie outra diretiva para, por exemplo, Recursos.

Referência de permissões

As seguintes tabelas listam todas as permissões com dependências e filtros:

- Permissões por guia (na página 100)
- Permissões em objetos de automação (na página 106)
- Dependências de permissões (na página 109)
- Filtros para permissões (na página 112)

Permissões por guia

As ações selecionadas em diretivas do CA EEM predefinidas concedem permissões para guias, paletas, pastas e objetos de automação. As tabelas a seguir descrevem as permissões que cada ação concede aos grupos (identidades) nas diretivas de recursos correspondentes.

Se você criar diretivas personalizadas a partir dessas classes de recursos, use as tabelas correspondentes como um guia para atribuir permissões.

Guia Início

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Console_Login (Usuário)	Usuário de produto	Efetuar logon no CA Process Automation e usar a guia Início.

Guia Biblioteca

A tabela a seguir lista as permissões do nível mais baixo para o mais alto. Para exibir a guia Biblioteca, você deve ter as permissões LibraryBrowser_User e Environment_Library_User ou Environment_Library_Admin. Para obter mais informações, consulte Dependências de permissões (na página 109).

Chave de ação (Nome localizado)	**Classe de recurso da diretiva**	**Permissões**
LibraryBrowser_User (Usuário do Navegador da biblioteca)	LibraryBrowser (Navegador da biblioteca)	Exibir acesso à guia Biblioteca.
Object_List (Listar)	Objeto	■ Exibir pasta ou objeto de automação no Navegador da biblioteca. ■ Definir exibições personalizadas da biblioteca.
Environment_Library_User (Usuário)	Ambiente	Pré-requisito para muitas permissões na guia Operações. ■ Acesso aos orquestradores adicionados aos ambientes. ■ Exibir, exportar, pesquisar objetos de automação na guia Biblioteca se o acesso for definido.
Object_Read (Ler)	Objeto	Ir até um caminho de pasta e abrir qualquer objeto de automação no criador ou visualizador correspondente. *Implícito:* lista
Object_Edit (Editar)	Objeto	Editar uma pasta ou um objeto de automação em uma pasta. *Implícito:* leitura, lista
Object_Delete (Excluir)	Objeto	Excluir uma pasta ou excluir um objeto de automação adicionado a uma pasta. *Implícito:* excluir, leitura, lista
Object_Admin (Admin.)	Objeto	Criar uma pasta ou qualquer objeto de automação. *Implícito:* excluir, editar, leitura, lista
Environment_Library_Admin (Administrador de conteúdo)	Ambiente	Criar, excluir, editar, ler e listar em todos os objetos de automação na guia Biblioteca.

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Group_Config_Admin	Configuração do grupo	Acessar a guia Configuração do grupo. Consulte Permissões em objetos de automação (na página 106) para obter informações sobre permissões concedidas em operadores personalizados.

Guia Criador

Os usuários com acesso à guia Criador geralmente também recebem acesso à guia Biblioteca. Os criadores precisam, no mínimo, das seguintes permissões da guia Biblioteca para salvar um processo que estejam criando:

- LibraryBrowser_User
- Environment_Library_User
- Object_Edit (que inclui as permissões Object_List e Object_Read)

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Designer_User (Usuário do criador)	Designer	Exibir acesso à guia Criador.

Guia Operações e paletas

Os criadores precisam de acesso à guia Operações no ambiente de criação; os usuários de produção precisam de acesso à guia Operações no ambiente de produção. Para exibir a guia Operações, você deve ter a permissão Environment_Library_User ou Environment_Library_Admin. Para obter mais informações, consulte Dependências de permissões (na página 109).

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Operations_Process_Watch (Exibição de processos)	Operações	■ Abrir a paleta Exibição de processos na guia Operações. ■ Exibir todos os processos no estado selecionado, programações ativas, operadores ativos e solicitações do usuário.

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Process_Monitor (Monitorar)	Processo	■ Abrir uma instância de processo em execução no Criador de processos. ■ Monitorar o andamento. ■ Definir pontos de interrupção. *Implícito:* lista
Process_Start (Iniciar)	Processo	Iniciar uma instância de processo. *Implícito*: monitorar, lista
Process_Control (Controlar)	Processo	Suspender, reiniciar, retomar ou cancelar instâncias de processo. *Implícito:* iniciar, monitorar, lista
Operations_Schedules (Programações)	Operações	Exibir o link Programações ativas na guia Operações.
Agenda_Control (Controlar)	Agenda	Ativar e desativar uma programação em um touchpoint. *Implícito:* leitura, lista
Operations_Datasets (Conjuntos de dados)	Operações	Abrir a paleta Conjuntos de dados na guia Operações.
Dataset_Inspect (Inspecionar)	Conjunto de dados	Exibir um objeto do conjunto de dados e ler os valores das variáveis no conjunto de dados. *Implícito:* lista
Dataset_Modify (Modificar)	Conjunto de dados	Criar, editar e excluir o objeto do conjunto de dados. *Implícito:* inspecionar, leitura, lista
Operations_Resources (Recursos)	Operações	Abrir a paleta Recursos na guia Operações.
Resources_Control (Controlar)	Recursos	■ Bloquear, desbloquear, assumir, retornar ou adicionar um parâmetro a um recurso. ■ Adiciona ou remove uma unidade do recurso. *Implícito:* leitura, lista
Operations_User_Requests (Solicitações do usuário)	Operações	Abrir a paleta Solicitações do usuário na guia Operações.

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Operations_Content_Packages (Pacotes de conteúdo)	Operações	Abrir a paleta Pacotes de conteúdo na guia Operações.
Operations_Task_List (Lista de tarefas)	Operações	■ Usar o link Lista de tarefas da guia Operações e exibir as tarefas para você, o seu grupo ou qualquer grupo. ■ Acessar suas tarefas a partir da guia Início.
StartRequestForm_Dequeue (Retirar da fila)	Formulário de solicitação inicial	Retirar da fila um processo que um formulário de solicitação inicial colocou na fila. *Implícito:* iniciar, lista
StartRequestForm_Start (Iniciar)	Formulário de solicitação inicial	Iniciar uma tarefa que um formulário de solicitação inicial define. *Implícito:* lista
Execute	Segurança do TouchPoint	Executar scripts ou programas em operadores. O produto deriva os operadores afetados de categorias do operador especificadas. O impacto ocorre quando o destino é um touchpoint especificado em um ambiente especificado.

Guia Relatórios

A tabela a seguir lista as ações relevantes para o uso da guia Relatórios.

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Reports_User (Usuário de relatórios)	Relatórios	■ Abrir a guia Relatórios. ■ Fazer upload de relatórios personalizados. ■ Exibir ou excluir os relatórios predefinidos, compartilhados ou particulares.

Guia Configuração e paletas

A tabela a seguir lista as ações que afetam as permissões na guia Configuração. Para exibir o Navegador de configuração na guia Configuração, é necessário ter a permissão Client_Configuration_User. Para obter mais informações, consulte Dependências de permissões (na página 109).

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Client_Configuration_User (Exibir Navegador de configuração)	Navegador de configuração	Exibir o Navegador de configuração na guia Configuração.
Environment_Configuration_Admin (Administrador de configuração)	Ambiente	■ Adicionar novo grupo, Adicionar touchpoint e Adicionar grupo de hosts no Navegador de configuração. ■ Editar a configuração em nível de ambiente, incluindo segurança, propriedades, categorias do operador, grupos de operador personalizado e acionadores.
Domain_Admin (Administrador)	Domain	■ Na paleta Navegador de configuração, bloquear ou desbloquear o domínio, adicionar Ambiente, chamar Remoção de agente em massa e chamar Remoção de touchpoint em massa. ■ Editar a configuração em nível de domínio, incluindo segurança, propriedades, categorias do operador, grupos de operador personalizado e acionadores. ■ Atualizar o conteúdo das pastas Recursos do orquestrador e Recursos do agente na paleta Gerenciar recursos de usuário.
Configuration_User_Resources (Recursos do usuário)	Navegador de configuração	Abrir a paleta Gerenciar recursos de usuário na guia Configuração e atualizar o conteúdo da pasta Recursos do usuário.
Configuration_Installations (Instalações)	Navegador de configuração	Abrir a paleta Instalação na guia Configuração e iniciar a instalação de um agente, orquestrador ou nó de agrupamento de um orquestrador.

Mais informações:

Dependências de permissões (na página 109)

Permissões em objetos de automação

A tabela a seguir descreve as permissões que você pode conceder a vários objetos de automação por meio de diretivas personalizadas do CA EEM. É possível conceder permissões para todos os grupos de aplicativos do CA EEM. O acesso a objetos de automação e pastas em qualquer orquestrador em um ambiente exige acesso de usuário ou administrador de conteúdo na diretiva de ambiente. O ambiente é a classe de recurso pai para as classes de recursos para objetos de automação.

Algumas permissões implicitamente incluem outras permissões. Quando você seleciona uma determinada permissão, permissões implícitas são selecionadas simultaneamente. Quando você concede uma permissão explícita, são implicitamente concedidas todas as outras permissões abaixo dela na hierarquia de permissões.

Quando você nega uma permissão implícita, nega todas as outras permissões acima dela na hierarquia de permissões. A lista de permissões está implícita para todas as outras permissões e não depende de nenhuma outra permissão. Você pode negar todas as permissões para um grupo em uma pasta com uma diretiva personalizada de objeto que nega permissões com Listar. Revogar uma Lista de permissões revoga todas as outras permissões em um objeto de automação. Entretanto, revogar outras permissões nunca revoga a permissão Listar.

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Object_Admin (Admin.)	Objeto	Criar uma pasta ou qualquer objeto de automação **Implícito:** excluir, editar, ler, listar
Object_Delete (Excluir)	Objeto	Excluir uma pasta ou excluir um objeto de automação adicionado a uma pasta. **Implícito:** editar, ler, listar
Object_Edit (Editar)	Objeto	Editar uma pasta ou editar um objeto de automação em uma pasta. **Implícito:** leitura, lista
Object_Read (Ler)	Objeto	Navegar até um caminho de pasta e abrir qualquer objeto de automação no criador ou visualizador correspondente. **Implícito:** lista

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
Object_List (Listar)	Objeto	Exibir uma pasta ou um objeto de automação no Navegador da biblioteca. Define exibições personalizadas da biblioteca.
Environment_Library_Admin (Administrador de conteúdo)	Ambiente	Criar, excluir, editar, ler e listar todos os objetos de automação.
Environment_Library_User (Usuário)	Ambiente	Exibir, exportar e pesquisar objetos de automação se o acesso for definido. **Observação**: implicitamente herdável pelas classes de recurso de objetos de automação
Agenda_Control (Controlar)	Agenda	Ativar e desativar uma programação em um touchpoint. **Implícito:** leitura, lista
Dataset_Modify (Modificar)	Conjunto de dados	Criar, editar e excluir o objeto do conjunto de dados. **Implícito:** inspecionar, ler, listar
Dataset_Inspect (Inspecionar)	Conjunto de dados	Exibe um objeto do conjunto de dados e lê os valores das variáveis no conjunto de dados. **Implícito:** lista
Process_Control (Controlar)	Processo	Suspender, reiniciar, continuar ou anular instâncias de um processo. **Implícito:** iniciar, monitorar, listar
Process_Start (Iniciar)	Processo	Iniciar uma instância de um processo. **Implícito**: monitorar, listar
Process_Monitor (Monitorar)	Processo	Abra uma instância em execução de um processo no Criador de processos, monitore o andamento e defina os pontos de interrupção. **Implícito:** lista
Resources_Control (Controlar)	Recursos	Bloquear, desbloquear, assumir, retornar ou adicionar um parâmetro a um recurso. Adiciona ou remove uma unidade do recurso. **Implícito:** leitura, lista
StartRequestForm_Dequeue (Retirar da fila)	Formulário de solicitação inicial	Permite retirar da fila um processo que um formulário de solicitação inicial colocou em fila. **Implícito:** iniciar, lista

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Permissões
StartRequestForm_Start (Iniciar)	Formulário de solicitação inicial	Iniciar uma tarefa que um formulário de solicitação inicial definiu. **Implícito:** lista
Execute	Segurança do TouchPoint	Executar scripts ou programas em operadores derivados de categorias de operadores especificadas que usam como destino touchpoints especificados em um determinado ambiente.
Group_Config_Admin	Configuração do grupo	Definir parâmetros para um grupo de operadores personalizado ao definir um operador personalizado. **Siga estas etapas:** 1. Bloquear o grupo de operadores personalizados na guia Configuração do grupo. 2. Adicionar páginas e variáveis. 3. Salvar a configuração. 4. Desbloquear o grupo de operadores personalizados. O desbloqueio publica a configuração do grupo de operadores personalizados nomeado. A publicação disponibiliza a configuração do grupo na guia Módulos do Navegador de configuração, nos níveis de domínio e ambiente.

Mais informações:

Dependências de permissões (na página 109)

Dependências de permissões

A tabela a seguir descreve a ação da classe de recursos dependente (permissão) para cada ação da classe de recursos nas diretivas predefinidas do CA EEM para o CA Process Automation.

Considere as dependências quando você atribuir apenas grupos personalizados (sem PAMUsers) a contas de usuário.

Conforme resumido na tabela, é possível atribuir uma Chave de ação em uma diretiva personalizada de uma classe de recurso a um grupo personalizado. Se você criar uma diretiva personalizada, atribua o grupo personalizado a uma chave de ações dependentes.

Chave de ação (Nome localizado)	Classe de recurso da diretiva personalizada	Chave de ações dependentes (Nome localizado)
Console_Login (Usuário)	Usuário de produto	
Reports_User (Usuário de relatórios)	Relatórios	Console_Login (Usuário)
Environment_Library_User (Usuário)	Ambiente	Console_Login (Usuário)
Environment_Library_Admin (Content Administrator)	Ambiente	Console_Login (Usuário)
Environment_Configuration_Admin (Configuration Administrator)	Ambiente	Console_Login (Usuário)
Domain_Admin (Administrator)	Domain	Console_Login (Usuário)
Client_Configuration_User (View Configuration Browser)	Navegador de configuração	Console_Login (Usuário)
Configuration_User_Resources (Recursos do usuário)	Navegador de configuração	■ Console_Login (Usuário) ■ Client_Configuration_User (View Configuration Browser) ■ Domain_Admin (Administrador) para acessar as pastas Recursos do agente e Recursos do orquestrador.
Configuration_Installations (Instalações)	Navegador de configuração	Console_Login (Usuário)
LibraryBrowser_User (Usuário do navegador da biblioteca)	Navegador da biblioteca	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ou Environment_Library_Admin (Administrador de conteúdo)

Chave de ação (Nome localizado)	Classe de recurso da diretiva personalizada	Chave de ações dependentes (Nome localizado)
Operations_User_Requests (Solicitações do usuário)	Operações	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ou Environment_Library_Admin (Administrador de conteúdo)
Operations_Process_Watch (Exibição de processos)	Operações	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ou Environment_Library_Admin (Administrador de conteúdo)
Operations_Task_List (Lista de tarefas)	Operações	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ou Environment_Library_Admin (Administrador de conteúdo)
Operations_Schedules (Programações)	Operações	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ou Environment_Library_Admin (Administrador de conteúdo)
Operations_Resources (Recursos)	Operações	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ou Environment_Library_Admin (Administrador de conteúdo)
Operations_Datasets (Conjuntos de dados)	Operações	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ou Environment_Library_Admin (Administrador de conteúdo)
Operations_Content Packages (Pacotes de conteúdo)	Operações	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ou Environment_Library_Admin (Administrador de conteúdo)

Chave de ação (Nome localizado)	**Classe de recurso da diretiva personalizada**	**Chave de ações dependentes (Nome localizado)**
■ Object_List (Lista) ■ Object_Read (Leitura) ■ Object_Edit (Editar) ■ Object_Delete (Excluir) ■ Object_Admin (Admin)	Objeto	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário)
Agenda_Control (Controle)	Agenda	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ■ Object_List (Listar) com recurso/*pasta* **Observação:** se o objeto for criado na pasta raiz, Object_List não é necessário.
■ Dataset_Inspect (Inspect) ■ Dataset_Modify (Modify)	Conjunto de dados	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ■ Object_List (Listar) com recurso/*pasta* **Observação:** se o objeto for criado na pasta raiz, Object_List não é necessário.
■ Process_Control (Controle) ■ Process_Monitor (Monitor) ■ Process_Start (Iniciar)	Processo	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ■ Object_List (Listar) com recurso/*pasta* **Observação:** se o objeto for criado na pasta raiz, Object_List não é necessário.
Resources_Control (Controle)	Recursos	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ■ Object_List (Listar) com recurso/*pasta* **Observação:** se o objeto for criado na pasta raiz, Object_List não é necessário.

Chave de ação (Nome localizado)	**Classe de recurso da diretiva personalizada**	**Chave de ações dependentes (Nome localizado)**
■ StartRequestForm_Start (Iniciar) ■ StarRequestForm_Dequeue (Retirar da fila)	Formulário de solicitação inicial	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ■ Object_List (Listar) com recurso/*pasta* **Observação:** se o objeto for criado na pasta raiz, Object_List não é necessário.
Execute	Segurança do touchpoint	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ■ Object_List (Listar) com recurso/*pasta* **Observação:** se o objeto for criado na pasta raiz, Object_List não é necessário.
Group_Config_Admin	Configuração do grupo	■ Console_Login (Usuário) ■ Environment_Library_User (Usuário) ■ Object_List (Listar) com recurso/*pasta* ■ Object_Edit (Editar) com recurso/*pasta*

Filtros para permissões

O CA EEM define as permissões como ações da classe de recurso. É possível, opcionalmente, usar filtros para limitar as ações que você permite a um grupo ou usuário. Por exemplo, você pode criar um escopo das permissões, para que elas se apliquem ao grupo atribuído somente no ambiente configurado.

O seguinte exemplo de Filtros ilustra o uso de AMBIENTE como o atributo nomeado para o filtro. As diretivas que são definidas como diretivas de acesso permitem adicionar filtros.

Filters

Logic	(	Left type/value	Operator	Right type/value	)	Actions
NONE		named attribute ENVIRONMENT	STRING EQUAL ==	value Default Environment		

As ações na tabela abaixo pertencem a diretivas com base na classe do recursos referenciada.

Chave de ação (Nome localizado)	Classe de recurso da diretiva	Atributo nomeado para filtro
Object_List (Lista) Object_Read (Leitura) Object_Edit (Editar) Object_Delete (Excluir) Object_Admin (Admin)	Objeto	SECURITY_CONTEXT_ID SECURITY_CONTEXT_GRP AMBIENTE OBJECT_TYPE
Agenda_Control (Controle)	Agenda	AMBIENTE
Dataset_Inspect (Inspect) Dataset_Modify (Modify)	Conjunto de dados	AMBIENTE
Process_Control (Controle) Process_Monitor (Monitor) Process_Start (Iniciar)	Processo	SECURITY_CONTEXT_ID SECURITY_CONTEXT_GRP AMBIENTE
Resources_Control (Controle)	Recursos	AMBIENTE
StartRequestForm_Start (Iniciar) StarRequestForm_Dequeue (Retirar da fila)	Formulário de solicitação inicial	AMBIENTE
Execute	Segurança do TouchPoint	AMBIENTE TOUCHPOINT

Como realizar a transição de funções utilizadas no Active Directory para o CA EEM

Se você já usou o Microsoft Active Directory (AD) ou o LDAP para autenticação e autorização, pode fazer a transição para o CA EEM com qualquer uma das seguintes abordagens:

- Crie contas de usuário. Atribua um dos grupos padrão para cada conta.

  Observação: consulte Revisar permissões para grupos padrão (na página 48).

- Aponte para o AD como um armazenamento de usuários externo.

  Observação: consulte o tópico Gerenciar acesso a contas de usuários de referência (na página 62). Consulte o tópico Integrar o Active Directory ao CA EEM.

- Crie grupos personalizados que reflitam suas funções do AD. Adicione esses grupos a diretivas do CA EEM e conceda as permissões necessárias. Crie contas de usuário. Atribua um de seus grupos personalizados para cada conta. Esta seção trata dessa abordagem.

Suponha que você tenha definido as configurações de segurança do domínio no Active Directory com estes grupos: ITPAMAdmins, ITPAMUsers, ConfigAdmin, ContentAdmin e EnvironmentUser.

Configurações de segurança do domínio

Administrador do domínio	ITPAMAdmins
Usuário do CA IT PAM	ITPAMUsers
Administrador de configuração do ambi...	ConfigAdmin
Administrador de conteúdo do ambiente	ContentAdmin
Usuário do ambiente	EnvironmentUser

Para migrar o acesso com base em função do Active Directory para o CA EEM manualmente, use o processo a seguir.

Siga estas etapas:

1. Migre o acesso baseado em função para usuários na função Administrador de domínio.

   Consulte Criar contas de usuário para administradores (na página 56).

2. Migre o acesso baseado em função para usuários na função Usuário do CA Process Automation.

   Consulte Criar contas de usuário com acesso básico (na página 58).

3. Migre o acesso baseado em função para usuários na função Administrador de configuração do ambiente, como se segue:

   a. Criar o grupo personalizado ConfigAdmin (na página 115).

   b. Conceder permissões para o grupo personalizado ConfigAdmin (na página 116).

   c. Criar contas de usuário para administradores de configuração do ambiente (na página 117).

4. Migre o acesso baseado em função para usuários na função Administrador de conteúdo do ambiente, como se segue:

   a. Criar o grupo personalizado ContentAdmin (na página 117).

   b. Conceder permissões para o grupo personalizado ContentAdmin (na página 118).

   c. Criar contas de usuário para administradores de conteúdo do ambiente (na página 118).

5. Migre o acesso baseado em função para usuários na função Usuário do ambiente.

   Consulte Criar contas de usuário para usuários de produção (na página 58).

Criar o grupo personalizado ConfigAdmin

É possível criar um grupo ConfigAdmin personalizado para usuários na função Administrador de configuração do ambiente.

Siga estas etapas:

1. Navegue até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades, clique em Grupos, e clique em Novo grupo de aplicativos.
3. Digite **ConfigAdmin** como o nome do grupo ou digite um nome de sua escolha.
4. (Opcional) Insira uma descrição para o grupo.
5. Clique em Salvar.

   Observação: não adicione uma associação ao grupo de aplicativos.

6. Clique em Fechar.

Conceder permissões ao grupo de administradores de configuração do ambiente

Você pode conceder permissões ao grupo personalizado Administradores de configuração do ambiente adicionando esse grupo às diretivas selecionadas e selecionando as ações necessárias.

Siga estas etapas:

1. Efetue logon no aplicativo do CA Process Automation no CA EEM.
2. Clique na guia Manage Access Policies.
3. Conceda ao grupo ConfigAdmin a capacidade de efetuar logon no CA Process Automation e exibir a Página inicial.
    a. Clique no link Usuário do produto em Diretivas de acesso.
    b. Clique na diretiva de logon de usuário PAM40.
    c. Selecione Grupo de aplicativos para tipo em Digitar/pesquisa identidades, clique em Pesquisar identidades e em Pesquisar.
    d. Selecione o grupo personalizado, ConfigAdmin, e clique na seta para baixo.
    e. Selecione Console_Login para a nova identidade.
    f. Clique em Salvar.
4. Conceda ao grupo ConfigAdmins as permissões para bloquear um ambiente e executar qualquer ação que exija que o ambiente seja bloqueado.
    a. Clique no link Ambiente em Diretivas de acesso.
    b. Clique no link Diretiva de ambiente PAM40 na tabela de diretivas.
    c. Adicione as identidades. Pesquise grupos. Especifique Grupo de aplicativos por tipo, clique em Pesquisar identidades e em Pesquisar.
    d. Selecione ConfigAdmin e clique na seta para baixo.
    e. Selecione a permissão Environment_Configuration_Admin (Administrador da configuração).
    f. Clique em Salvar. Clique em Fechar.
5. Conceda ao grupo ConfigAdmin as permissões para acessar a guia Configuração e instalar orquestradores e agentes.
    a. Clique em Navegador de configuração.
    b. Clique na diretiva de configuração PAM40.
    c. Procure ConfigAdmin e adicione o grupo às Identidades selecionadas.
    d. Selecione Client_Configuration_User (Exibir Navegador de configuração) e Configuration_Installations.
6. Clique em Fechar.

Criar contas de usuário para administradores de configuração do ambiente

Você pode criar contas de usuário para pessoas que executam a função de Administrador de configuração do ambiente.

Siga estas etapas:

1. Navegue até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar identidades.
3. Clique em Novo usuário.
4. Insira a ID de usuário como o nome.
5. Clique em Adicionar detalhes do usuário do aplicativo.
6. Selecione o grupo ConfigAdmin e clique na seta para a direita.
7. Insira os detalhes do usuário global conforme necessário.
8. Insira uma senha temporária duas vezes na seção Autenticação.
9. Clique em Salvar.
10. Repita esse procedimento para cada usuário na função Administrador de configuração do ambiente.

Criar o grupo personalizado ContentAdmin

Você pode criar um grupo personalizado no CA EEM denominado ContentAdmin para usuários na função Administrador de conteúdo do ambiente. Você pode basear esse grupo no grupo Criador padrão para obter automaticamente as permissões atribuídas ao grupo Criador.

Siga estas etapas:

1. Efetue logon no aplicativo do CA Process Automation no CA EEM.
2. Clique na guia Gerenciar identidades.
3. Clique em grupos.
4. Clique em Novo grupo de aplicativos.
5. Digite ContentAdmin como o nome do grupo e, se desejar, uma descrição
6. Selecione Criadores em Grupos de usuários disponíveis e clique na seta para a direita a fim de mover Criadores para Grupos de usuários selecionados.
7. Clique em Salvar.
8. Clique em Fechar.

Conceder permissões para o grupo personalizado ContentAdmin

É possível conceder permissões ao grupo Administrador de conteúdo do ambiente adicionando esse grupo às diretivas padrão e selecionando as permissões necessárias. Muitas das permissões de diretiva já foram concedidas a ContentAdmin porque você o baseou no grupo padrão Criadores. Adicione os direitos de administrador às pastas, aos objetos de automação e aos editores na guia Biblioteca.

Siga estas etapas:

1. Efetue logon no aplicativo do CA Process Automation no CA EEM.
2. Clique na guia Manage Access Policies.
3. Clique no link Ambiente em Diretivas de acesso.
4. Clique no link Diretiva de ambiente PAM40 na tabela de diretivas.
5. Adicione as identidades. Pesquise grupos. Especifique Grupo de aplicativos por tipo, clique em Pesquisar identidades e em Pesquisar.
6. Selecione ContentAdmin e clique na seta para baixo.
7. Selecione as permissões Environment_Library_Admin (Administrador de conteúdo).
8. Clique em Salvar.
9. Clique em Fechar.

Criar contas de usuário para administradores de conteúdo do ambiente

Você pode criar contas de usuário para pessoas que executam a função de Administrador de conteúdo do ambiente.

Siga estas etapas:

1. Navegue até o CA EEM e efetue logon. (na página 46)
2. Clique na guia Gerenciar identidades.
3. Clique em Novo usuário.
4. Digite a ID de usuário como o nome.
5. Clique em Adicionar detalhes do usuário do aplicativo.
6. Selecione o grupo ContentAdmin e clique na seta para a direita.
7. Digite os detalhes do usuário global conforme necessário.
8. Digite uma senha temporária duas vezes na seção Autenticação.
9. Clique em Salvar.
10. Repita esse procedimento para cada usuário na função Administrador de conteúdo do ambiente.

Segurança do touchpoint com o CA EEM

A finalidade da segurança do touchpoint é limitar o acesso a hosts essenciais aos negócios ou hosts com informações altamente confidenciais a um grupo de usuários com altos privilégios.

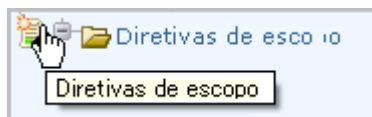
Esta seção se aplicará somente se você tiver ativado a segurança do touchpoint para touchpoints em um ou mais ambientes.

- Para determinar se a segurança do touchpoint está ativada em touchpoints mapeados para hosts candidatos, verifique a configuração de segurança do touchpoint nas propriedades do touchpoint. Se a opção Herdar do ambiente estiver marcada, considere a possibilidade de alterar a configuração para Ativado.
- Para determinar se um touchpoint específico está mapeado para um host que precisa de proteção está protegido, revise os filtros nas diretivas Segurança do touchpoint.

Conceder a usuários acesso ao CA EEM para definir diretivas de segurança do touchpoint

Por padrão, o usuário EiamAdmin é o único que pode efetuar logon no CA EEM. Se você usar uma abordagem de segurança do touchpoint com base em diretivas, poderá autorizar determinados usuários a criar diretivas de segurança do touchpoint no CA EEM. Autorize os criadores de conteúdo que criam processos com operadores que são executados em touchpoints mapeados para hosts que possuem um alto valor comercial. Esses touchpoints podem ser protegidos por meio de diretivas de segurança do touchpoint que especifiquem os usuários que têm permissão para executar esses operadores.

Para conceder aos criadores de diretivas especificados acesso ao CA EEM e autorização para criar diretivas com a classe de recursos Segurança do touchpoint

1. Efetue logon no aplicativo do CA Process Automation no CA EEM.
2. Clique na guia Manage Access Policies.
3. Clique em Nova diretiva de escopo.

4. Preencha a seção Geral da seguinte maneira:

   Nome

   Especifica o nome dessa diretiva de escopo. Por exemplo, Usuários criando diretivas de segurança do touchpoint.

   Descrição

   (Opcional) Fornece uma descrição resumida. Por exemplo, Permite que usuários especificados criem diretivas personalizadas apenas com a classe de recursos Segurança do touchpoint.

   Calendário e nome da classe de recursos

   Ignore a opção Calendário e aceite a entrada padrão SafeObject para o nome da classe de recursos.

   Tipo

   Especifique a lista de controle de acesso.

   Observação: uma mensagem é exibida informando que alterar o tipo de diretiva redefine alguns filtros. Clique em OK.

5. Em Identidades, adicione os nomes de todos os usuários que criam processos para os quais a segurança do touchpoint se aplica. Os usuários adicionados a essa diretiva recebem acesso de logon ao CA EEM e a capacidade de criar diretivas de segurança do touchpoint. Uma diretiva de segurança do touchpoint especifica os usuários a serem autorizados a executar operadores a partir de uma determinada categoria de operadores em um touchpoint especificado.

   Observação: se desejar testar essa diretiva, crie um usuário com o grupo de usuários padrão e adicione o nome desse usuário aqui. Depois de salvar essa diretiva, efetue logon no CA EEM com seu nome de usuário de teste. Observe que a única coisa que você pode fazer no CA EEM é criar uma diretiva com a classe de recursos Touchpoint.

   a. Aceite Usuário como Tipo ou selecione outro valor.

   b. Clique no link Procurar identidades.

   c. Digite os critérios de pesquisa que incluem o usuário ou o grupo planejado e clique em Pesquisar.\

   d. Selecione um usuário ou grupo da lista exibida de identidades disponíveis e clique na seta para a direita.

      O usuário ou o grupo selecionado é exibido na lista de identidades selecionadas.

   e. Repita este processo para cada usuário que deseja autorizar a criar diretivas de segurança do touchpoint.

6. Configure a lista de controle de acesso da seguinte maneira:

   a. Selecione cada um dos recursos a seguir na lista suspensa e clique em Adicionar para adicioná-los à lista.

      ■ ApplicationInstance

      ■ Diretiva

      ■ Usuário

      ■ GlobalUser

      ■ UserGroup

      ■ GlobalUserGroup

   b. Clique em ler para todos os recursos. Clique em gravar para Diretiva

   c. Clique em Filtros.

   d. Para Diretiva, selecione o atributo nomeado na primeira lista suspensa. No campo abaixo do atributo nomeado, digite ResourceClassName. No campo de valor após EQUAL, digite TouchPointSecurity. Não digite um espaço entre TouchPoint e Security.

Configuração da lista de controle de acesso

Recursos	Ações	Filtros
Adicionar recurso: ApplicationInstance	read (ler) write (gravar)	
ApplicationInstance	☑ ☐	valor / STRING / EQUAL == / valor
Policy	☑ ☑	atributo nomeado / ResourceClassName / STRING / EQUAL == / valor / TouchPointSecurity

   e. Não altere os demais campos da página de filtros.

7. Clique em Salvar.

8. Verifique se a configuração da lista de controle de acesso corresponde exatamente ao exemplo a seguir. O sistema adiciona um espaço entre TouchPoint e Security.

Configuração da lista de controle de acesso

Recursos	Ações	Filtros
Adicionar recurso: ApplicationInstance	read (ler) write (gravar)	
ApplicationInstance	☑ ☐	
Policy	☑ ☑	atributo nomeado: **ResourceClassName** == valor: **TouchPointSecurity**
User	☑ ☐	
GlobalUser	☑ ☐	
UserGroup	☑ ☐	
GlobalUserGroup	☑ ☐	

☐ **Tratar nomes de recursos como expressões regulares**

9. Verifique se sua diretiva se parece com o seguinte exemplo. No exemplo, as colunas ausentes indicam que ResourceClassName é SafeObject, o valor Opções é Concessão explícita, e Identidades é sua lista de usuários. Esses são os usuários que criam processos para a segurança do touchpoint e criam uma diretiva associada.

Diretivas de escopo

Nome/Descrição	Ações	Recursos	Filtros
Users Defining Touchpoint Security Policies Enables specified users to create custom policies only with the TouchPoint Security resource class.	read write	ApplicationInstance Policy GlobalUser User UserGroup GlobalUserGroup	ONDE (req:resource == val:ApplicationInstance ApplicationInstanc E req:action {} val:read) ApplicationInstanc OU (req:resource == val:Policy Policy E req:action {} val:read,write Policy E name:ResourceClassName == val:TouchPointSecurity) Policy OU (req:resource == val:User User E req:action {} val:read) User OU (req:resource == val:GlobalUser GlobalUser E req:action {} val:read) GlobalUser OU (req:resource == val:UserGroup UserGroup E req:action {} val:read) UserGroup OU (req:resource == val:GlobalUserGroup GlobalUserGroup E req:action {} val:read) GlobalUserGroup

Sobre a segurança do touchpoint

A segurança do touchpoint permite proteger touchpoints associados a hosts essenciais aos negócios e hosts que contenham dados confidenciais. Você pode proteger esses touchpoints contra o acesso não autorizado. É possível criar diretivas de touchpoint que especificam usuários selecionados ou um grupo com altos privilégios como as únicas identidades que podem executar um operador no destino. As políticas especificam as identidades que estão autorizadas a executar determinados operadores em touchpoints especificados. Os operadores que executam programas e scripts estão contidos em categorias de operadores especificadas.

Em resumo, as diretivas de segurança do touchpoint do CA EEM autorizam identidades especificadas a executar scripts em operadores de determinadas categorias em touchpoints específicos de um ambiente em particular.

Considere o seguinte trecho de exemplo de uma diretiva de segurança do touchpoint simples.

Identidades	Ações	Recursos	Filtros
ug:High-PrivilegedUsers	[Todas as ações]	✔ Comparar Regex Network Utilities Module Process Module File Module	ONDE (name:ENVIRONMENT == val:Production E (name:TOUCHPOINT == val:SensitiveHostTP1 OU name:TOUCHPOINT == val:SensitiveHostTP2 OU name:TOUCHPOINT == val:SensitiveHostTP3))

O exemplo é uma parte de uma diretiva. A diretiva permite que apenas usuários do grupo High-PrivilegedUsers executem qualquer operador a partir de categorias específicas em determinados touchpoints no ambiente de produção. O touchpoints de exemplo são nomeados SensitiveHostTP1, 2, e 3. As IDs do Access Control especificadas incluem os módulos Utilitários de rede e Processo (para a execução de comando). O módulo Arquivo* inclui o módulo Arquivo para o gerenciamento de arquivos e o módulo Transferência de arquivos.

Observação: consulte Identificar as IDs do Access Control para adicionar como recursos (na página 127).

Um processo com um destino de operador protegido por uma diretiva de segurança do touchpoint pode ser concluído com êxito apenas se for executado como um usuário autorizado. O usuário em nome do qual o processo é executado é especificado como uma Identidade na diretiva. A diretiva identifica os usuários por nome ou associação de grupo, os operadores por IDs do Access Control associadas às categorias de origens e os touchpoints por nome, ambiente ou ambos.

As diretivas de segurança do touchpoint protegem o acesso a hosts individuais de destino por meio do controle de quem executa os operadores em um touchpoint ou grupo de hosts específico. Uma instância de processo é executada em nome de um usuário. Quando o processo executa um operador em um touchpoint ou grupo de hosts especificado em uma diretiva de segurança do touchpoint do CA EEM, o CA EEM tenta autorizar esse usuário. O CA EEM verifica se o usuário está especificado como uma Identidade em uma diretiva de segurança do touchpoint para esse touchpoint. Se a instância de processo estiver sendo executada em nome de um usuário não autorizado, o operador irá falhar.

É possível especificar hosts confidenciais como touchpoints, touchpoints do proxy ou grupos de hosts.

Você pode limitar o acesso a hosts especificados para usuários com altos privilégios. É possível conceder acesso a um usuário ou grupo especificados que receberam o seguinte pré-requisito de acesso:

- Ação Console_Login (Usuário) concedida na diretiva de logon de usuário PAM40.
- Ação Environment_Library_User (Usuário) concedida na diretiva de ambiente PAM40.

Casos de uso: quando a segurança do touchpoint é necessária

A segurança do touchpoint é necessária nos seguintes casos:

- Um host em seu ambiente que pode ser um destino do operador contém informações confidenciais, como números do seguro social, números de cartão de crédito ou detalhes de sua saúde. Você deseja limitar o acesso a esse processo confidencial a uma única pessoa ou a um pequeno grupo com altos privilégios.

  O destino pode ser qualquer um dos seguintes hosts:

  - O host com um agente associado a um touchpoint.
  - O host com um agente associado a um touchpoint do proxy com uma conexão SSH a um host remoto.
  - O host com um agente associado a um grupo de hosts que faz referências e possui uma conexão a hosts remotos.

- Quando estiver executando um agente em um host, como o usuário raiz (UNIX), o administrador (Windows) ou um usuário com direitos específicos. Suponha que você tenha um motivo para executar todos os scripts e programas nesse agente na mesma identidade do próprio agente. Ou seja, você não deseja alternar para outro usuário que requeira credenciais. Para evitar um risco à segurança, é possível restringir usuários com poucos privilégios de executar scripts com a mesma identidade do agente, como o usuário raiz.

- Considere o caso em que você está aproveitando grupos de hosts que definem credenciais do sistema operacional padrão para executar operadores de execução de comando em sub-redes inteiras. Suponha que você tenha um motivo para executar todos os scripts e programas nesse grupo de hosts usando as credenciais do sistema operacional. Você deseja evitar um risco à segurança, proibindo que usuários com poucos privilégios criem e executem qualquer script usando credenciais do sistema operacional.

- Os usuários que executam um processo podem selecionar destinos de operador em tempo de execução para operadores que tenham uma variável no campo de destino. Um destino do operador geralmente é um touchpoint, embora possa ser um touchpoint do proxy, um FQDN ou um endereço IP referenciado por um grupo de hosts. Esse design flexível permite que qualquer usuário autorizado a executar o processo selecione um destino em tempo de execução.

  Um problema de segurança ocorre quando um touchpoint disponível requer limitações para seu acesso. Considere o caso em que um operador possa executar com êxito em dois touchpoints diferentes, e cada um deles representa um aplicativo do Service Desk. Um touchpoint representa um Service Desk criado para acesso geral, ao passo que o outro é criado apenas para administradores. A segurança do touchpoint permite que somente os administradores executem esse operador de exemplo no touchpoint criado para administradores. As políticas de segurança do touchpoint no CA EEM limitam o acesso.

A segurança do touchpoint também é útil para criadores de processos. Durante o desenvolvimento de processos, diferentes criadores instalam um agente em seus hosts pessoais e criam touchpoints para seus agentes. Eles normalmente não desejam que outros usuários executem operadores em seus hosts locais. A segurança do touchpoint pode fornecer essa proteção. Quando a segurança do touchpoint estiver configurada para estar ativa, a autorização para executar cada operador no destino selecionado é verificada no tempo de execução. A aplicação de diretivas restringe os usuários que executam um processo aos operadores apenas em touchpoints para os quais estão autorizados.

Limitar o acesso a hosts com informações confidenciais

A segurança do touchpoint responde pela necessidade de limitar o acesso aos hosts de negócios críticos e aos hosts nos quais você armazena informações confidenciais. A ilustração a seguir sugere uma abordagem para atingir essa meta de segurança.

Limitar o acesso a hosts com informações confidenciais

Administradores do CA EEM

Ir para o CA EEM e efetuar logon

Criar um grupo de usuários altamente privilegiados

Identificar touchpoints para hosts confidenciais

Identificar IDs de acesso de categorias com operadores que expõem dados

Criar uma diretiva de segurança de touchpoint com grupo, touchpoints e IDs de acesso

Ativar a segurança do touchpoint nos touchpoints selecionados

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Crie um grupo de usuários com altos privilégios.

   Consulte Criar o grupo personalizado ContentAdmin (na página 117).

3. Identifique os touchpoints associados a hosts confidenciais.

   Consulte Exibir os touchpoints e grupos de hosts de um agente selecionado (na página 210).

4. Identifique as categorias com operadores que expõem dados.

5. Identifique as ID do Access Control associadas a essas categorias.

   - Consulte Exemplo: proteger touchpoints essenciais (na página 131) para as IDs do Access Control IDs em consideração.
   - Localize descrições de cada categoria na seção Categorias de operadores e onde os operadores são executados (na página 311).
   - Consulte a *Referência de criadores de conteúdo* para obter descrições de operadores.

6. Crie uma diretiva de segurança do touchpoint com esse grupo, essas categorias de operador e esses touchpoints.

   Consulte Criar uma diretiva de segurança do touchpoint (na página 129).

7. Ativar a segurança do touchpoint nos touchpoints selecionados.

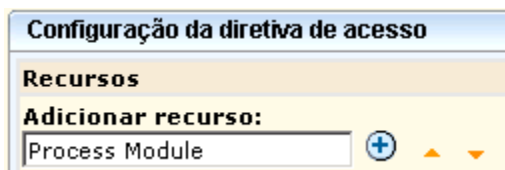
   - Consulte Configurar propriedades do touchpoint (na página 222).
   - Consulte Configurar propriedades do touchpoint do proxy (na página 243).
   - Consulte Configurar propriedades do grupo de hosts (na página 251).

Mais informações:

Abordagem para configurar a segurança do touchpoint (na página 149)

Identificar as IDs do Access Control para adicionar como recursos

Ao criar uma diretiva de segurança do touchpoint, não é preciso identificar diretamente os operadores que agem nos touchpoints que deseja proteger. Em vez disso, você identifica as categorias às quais esses operadores pertencem. Identifique as categorias, não por nome, mas pela ID do Access Control.

Configuração da diretiva de acesso
Recursos
Adicionar recurso:
Process Module

Nem todas as categorias contêm operadores que podem comprometer a segurança de um host com informações confidenciais. Avalie o impacto de operadores de adicionar recursos.

Você pode identificar a ID do Access Control para adicionar como um recurso a uma diretiva Segurança do touchpoint.

Siga estas etapas:

1. Navegue para o CA Process Automation e efetue logon (na página 18).
2. Clique na guia Configuração.
3. Selecione um agente no nó Agentes e, em seguida, selecione a guia Módulos.
4. Anote os nomes como eles aparecem na coluna ID do Access Control.

Propriedades | Módulos | Grupos de host... | Trilhas de audit...

Nome	Ativar/desativar	ID do Access Control
Bancos de dados	Herdar do ambiente	JDBC Module
Catalyst		Catalyst Module
Controle de processo		Workflow Module
Data/hora		Date-Time Module
Email	Herdar do ambiente	Mail Module
Execução de comando	Herdar do ambiente	Process Module
Gerenciamento de arq...	Herdar do ambiente	File Module
Gerenciamento de Java	Herdar do ambiente	JMX Module
Serviços de diretório	Herdar do ambiente	LDAP Module
Serviços web	Herdar do ambiente	SOAP Module
Transferência de arqu...	Herdar do ambiente	File Transfer Module
Utilitários	Herdar do ambiente	Utilities Module
Utilitários de rede	Herdar do ambiente	Network Utilities Module

Importante: a coluna ID do Access Control lista os nomes de módulo. Consulte essa lista ao digitar nomes de módulo selecionados no campo Recursos da diretiva de segurança do touchpoint.

Criar uma diretiva de segurança do touchpoint

Ao iniciar um processo, os devidos operadores são executados nos destinos especificados em uma determinada sequência. Uma diretiva de segurança do touchpoint personalizada concede permissão a usuários ou grupos especificados para executar operadores especificados em destinos especificados. Os administradores do CA EEM podem criar uma diretiva de segurança do touchpoint.

Siga estas etapas:

1. Vá até o CA EEM e efetue logon (na página 46).
2. Clique na guia Gerenciar diretivas de acesso.
3. Clique no botão Nova diretiva de acesso para Segurança do touchpoint em Diretivas de acesso.
4. No formulário da nova diretiva de acesso para a classe de recursos Segurança do touchpoint, digite um nome para a diretiva de segurança do touchpoint personalizada.

   A seção Digitar/procurar identidades permite especificar o usuário ou grupo de destino.
5. Selecione o tipo de destino para o qual deseja conceder acesso:
   - Selecione Usuário se o destino for um usuário global.
   - Selecione Grupo global se o destino for um grupo de um armazenamento de usuários de referência.
   - Selecione Grupo de aplicativos se o destino for um grupo personalizado que você definiu ou um grupo padrão.
6. Clique em Procurar identidades.
7. Selecione as identidades para as quais essa diretiva se aplica e clique na seta para baixo.

   A lista de Identidades selecionadas exibe sua seleção.
8. Selecione a ação Executar.

9. No campo Adicionar recurso, digite a ID do Access Control da Categoria do operador de origem que inclui os operadores para os quais essa diretiva se aplica. Por exemplo:

   - Digite **Process Module** para a categoria do operador Execução de comando.
   - Digite **File Module** para a categoria do operador Gerenciamento de arquivos.
   - Digite **File Transfer Module** para a categoria do operador Transferência de arquivos.
   - Digite **Network Utilities Module** para a categoria do operador Utilitários de rede.

   É possível digitar expressões regulares para cobrir as categorias do operador apropriadas e, em seguida, selecionar Tratar nomes de recursos como expressões regulares. Por exemplo, uma entrada Arquivo* incluiria operadores nas categorias Gerenciamento de arquivos e Transferência de arquivos.

10. Clique em Adicionar.
11. Adicione um filtro que especifica o ambiente que contém os destinos de diretiva:

    - Defina o atributo nomeado como Ambiente.
    - Defina o operador STRING como IGUAL A.
    - Defina o valor como o *nome_do_ambiente*.

12. Adicione outros filtros que especificam os destinos por nome de touchpoint:

    - Defina o atributo nomeado como Touchpoint.
    - Defina o operador STRING como IGUAL A.
    - Defina o valor como o *nome_do_touchpoint*.

13. Clique em Salvar.

    Se as diretivas de segurança do touchpoint estiverem configuradas para aplicação, o produto irá avaliar e impor a diretiva.

Exemplo: proteger touchpoints essenciais

A segurança do touchpoint garante que a execução de operadores em hosts essenciais aos negócios será limitada a um pequeno grupo de usuários com altos privilégios. A maneira mais fácil de proteger hosts confidenciais é criar uma diretiva de segurança do touchpoint e listar todos os touchpoints associados em um filtro. Em seguida, ativar a segurança do touchpoint na configuração de propriedades para cada um desses touchpoints.

Exemplo: configuração de segurança do touchpoint para um touchpoint essencial

O exemplo a seguir mostra as propriedades de um touchpoint selecionado. Quando a Segurança do touchpoint é definida como Ativado, o processo avalia cada tentativa de executar um operador nesse touchpoint em relação às diretivas de segurança do touchpoint.

Agentes
Propriedades
Trilhas de audit...
Recuperação automática de operadores
Herdar do ambiente
Segurança do touchpoint
Herdar do ambiente
Proxy Touchpoint

Exemplo: diretiva de segurança do touchpoint para touchpoints essenciais

Para garantir que apenas usuários com altos privilégios executem operadores em hosts confidenciais em seu ambiente de produção, crie uma diretiva de segurança do touchpoint. Na diretiva de segurança do touchpoint, adicione a ID do Access Control associada a cada categoria que contém os operadores que podem representar um risco. Adicione um filtro em seu ambiente. Adicione um filtro para cada touchpoint que faça referência a hosts confidenciais.

Considere o seguinte exemplo de diretiva de segurança global do touchpoint. A diretiva de exemplo concede ao grupo de usuários com altos privilégios autorização para executar scripts ou programas usando operadores de cinco categorias em touchpoints de alto risco. As IDs do Access Control representam as cinco categorias. Essa política é aplicável aos touchpoints especificados apenas no ambiente de produção.

Diretivas de acesso - "TouchPointSecurity"

Nome/Descrição	Nome da classe do recurso	Opções
Global TouchPoint Security Policy Authorizes High-Privileged group to execute risk posing Operators on Sensitive Hosts in Production.	TouchPointSecurity	Concessão explícita

Identidades	Ações	Recursos	Filtros
ug:High-PrivilegedUsers	Execute	Process Module File Module File Transfer Module JMX Module Network Utilities Module	ONDE name:ENVIRONMENT == val:Production E name:TOUCHPOINT == val:TP-SensitiveHost1 OU name:TOUCHPOINT == val:TP-SensitiveHost2 OU name:TOUCHPOINT == val:TP-SensitiveHost3 OU name:TOUCHPOINT == val:TP-SensitiveHost4 OU name:TOUCHPOINT == val:TP-SensitiveHostn

Exemplo: proteger o touchpoint para o host

Suponha que você instale um agente em um host e não deseja que ninguém além de você execute os operadores nesse host. Para usar a segurança do touchpoint para proteger um host que é essencial para você, considere a possibilidade de executar as tarefas necessárias na sequência a seguir.

1. Instale um agente no host.
2. Associe a esse host um touchpoint em um ambiente especificado.
3. Crie uma diretiva de segurança do touchpoint que liste você como a Identidade. Adicione a ID do Access Control a cada categoria com operadores que podem ser executados em touchpoints associados a agentes.
4. Configure a segurança do touchpoint como Ativada em propriedades do touchpoint para esse host.

Exemplo: definir a segurança do touchpoint como Ativada no touchpoint do PC

O parâmetro de segurança do touchpoint para o touchpoint selecionado, MyPC-TP, é definido como Ativado.

Agentes | Propriedades | Trilhas de audit...

Recuperação automática de operadores

Herdar do ambiente

Segurança do touchpoint

Herdar do ambiente

Proxy Touchpoint

Exemplo: criar uma diretiva de segurança do touchpoint que permite que apenas eu execute os operadores no touchpoint do PC

No seguinte exemplo, suponha que o host protegido pertence a um usuário chamado MyPCowner. Observe que MyPCowner é a única Identidade autorizada a executar operadores no touchpoint, MyPC-TP. Aqui, as IDs do Access Control estão associadas a todas as categorias com os operadores que podem ser executados em um host do agente. Nesse caso, as referências incluem as categorias de operadores que não fazem alterações no host. A ideia nesse exemplo é que o usuário não deseja que usuários externos acessem o host associado com o touchpoint MyPC-TP. Apenas MyPCowner pode executar processos em MyPC-TP quando a segurança do touchpoint está ativada.

Nome/Descrição	Nome da classe do recurso	Opções
Secure TP My PC	TouchPointSecurity	Concessão explícita

O nome de touchpoint é especificado como o valor no filtro.

Identidades	Ações	Recursos	Filtros
MyPCOwner	Execute	Process Module JDBC Module LDAP Module Mail Module File Module File Transfer Module JMX Module Network Utilities Module Utilities Module SOAP Module	**ONDE** name:ENVIRONMENT == val:Test **E** name:TOUCHPOINT == val:MyPC-TP

Autorizando ações no tempo de execução com o CA EEM

O CA Process Automation fornece um controle de acesso refinado sobre operações e ações do usuário em objetos de automação específicos, como processos, conjuntos de dados, calendários e programações. O controle inclui direitos tradicionais de leitura/gravação e direitos de iniciar um processo e monitorar suas instâncias. Os direitos de acesso são aplicados em todas as interfaces externas, incluindo serviços Web e interface de usuário do CA Process Automation. Além disso, o CA Process Automation fornece maneiras para proteger as operações em hosts de destino de modo que apenas usuários autorizados possam executá-las.

Para limitar quem pode executar qualquer uma das seguintes ações no tempo de execução, crie uma diretiva do CA EEM e especifique os usuários ou grupos a serem autorizados.

- Execute scripts ou programas em operadores derivados de categorias especificadas que têm como destino touchpoints especificados em um ambiente especificado.
- Controle uma programação, incluindo ativar e desativar.
- Inspecione ou modifique um conjunto de dados.
- Controle uma instância de processo, incluindo suspender, reiniciar, retomar e anular.
- Controle um recurso, incluindo bloquear, desbloquear, assumir, retornar ou adicionar uma variável para um recurso. Adiciona ou remove uma unidade do recurso.
- Retire da fila ou inicie um formulário de solicitação inicial.

Além disso, você pode criar uma diretiva que autoriza direitos de leitura/gravação em qualquer outro objeto de automação.

Alterar a propriedade para a automação de objetos

O usuário que cria um objeto de automação ou pasta é, por padrão, o proprietário. O proprietário tem controle total sobre o objeto de automação ou a pasta. Um proprietário pode alternar a propriedade para outro usuário do CA Process Automation.

Observação: a permissão Environment_Content_Administrator do CA EEM concede controle total sobre todos os objetos de automação e pastas. Todos os administradores que pertencem ao grupo PAMAdmins têm esta permissão.

Se você ativar a segurança em tempo de execução, apenas o proprietário do processo (ou um administrador) poderá iniciar esse processo.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Selecione um ou mais objetos, incluindo as pastas.
3. Clique no botão Definir proprietário, na barra de ferramentas.
4. Na lista Usuários disponíveis, selecione a conta de usuário a ser definida como o novo proprietário. Use a pesquisa para encontrar contas de usuário correspondentes.
5. Clique em Salvar e fechar.

Capítulo 5: Administrar o domínio do CA Process Automation.

No CA Process Automation, o domínio abrange todo o sistema. A administração do domínio inclui todas as tarefas executadas somente por um administrador com direitos de administrador do domínio. As tarefas incluem a adição de ambientes, a remoção de agentes e touchpoints não utilizados em massa e a configuração de segurança, propriedades, categoria de operador e disparadores no nível de domínio. Esse capítulo refere-se apenas às tarefas executadas durante a configuração inicial de um CA Process Automation recém-instalado. Os capítulos subsequentes referem-se às tarefas que são normalmente executadas durante o desenvolvimento de conteúdo.

Esta seção contém os seguintes tópicos:

Bloquear o domínio

Os administradores podem bloquear o domínio. Um bloqueio protege o domínio contra atualizações simultâneas feitas por vários usuários. Antes de fazer qualquer alteração de configuração no nível do domínio, bloqueie o domínio.

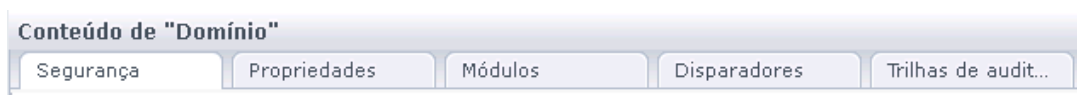
Siga estas etapas:

1. Clique na guia Configuração.
2. Selecione Domínio na paleta Navegador de configuração e clique em Bloquear.

Quando você concluir as alterações de configuração, selecione Domínio e clique em Desbloquear.

Configurar o conteúdo do domínio

Quando você seleciona Domínio no Navegador de configuração, as seguintes guias são exibidas em Conteúdo do "domínio":

Conteúdo de "Domínio"
Segurança | Propriedades | Módulos | Disparadores | Trilhas de audit...

- Segurança

  Consulte Configurar as definições de segurança do CA EEM para o domínio (na página 140).

- Propriedades

  Consulte Configurar propriedades do domínio (na página 146).

- Módulos

  Consulte Configurando categorias do operador (na página 270). Este tópico é seguido pelo procedimento de configuração para cada categoria do operador. Uma descrição de cada categoria precede cada procedimento de configuração.

- Gatilhos

  Consulte Como configurar e usar disparadores (na página 314). Este tópico é seguido por detalhes de configuração para cada tipo de disparador.

- Trilhas de auditoria

  Consulte Exibir a trilha de auditoria do domínio (na página 335).

Mais informações:

Mantendo o domínio (na página 381)

Sobre a herança de configuração

A configuração no nível de domínio inclui os seguintes tipos de configurações:

- Segurança
- Propriedades
- Categorias do operador
- Gatilhos

Objetos descendentes do domínio incluem o ambiente padrão, ambientes definidos pelo usuário, o orquestrador de domínio e agentes. Objetos descendentes de um ambiente incluem orquestradores definidos pelo usuário, touchpoints, incluindo touchpoints do proxy, e grupos de hosts.

Algumas definições configuradas no nível de domínio são, por padrão, herdadas por todos ou por objetos descendentes específicos dentro do domínio. Por exemplo, todos os ambientes podem herdar as configurações de categoria do operador do domínio. Os orquestradores podem herdar as configurações de categoria do operador de seu ambiente.

Como os agentes operam entre ambientes, a herança poderá ser diretamente por meio do domínio ou do ambiente, dependendo da configuração do ambiente. As configurações de categoria do operador podem ser substituídas no nível do agente. Agentes herdam a configuração da propriedade da frequência dos sinais de monitoramento diretamente do domínio.

Normalmente, as configurações são herdadas por padrão. Gatilhos são uma exceção. Configurações de gatilhos são desativadas por padrão em níveis inferiores, mas podem ser herdadas depois de ser ativadas.

Configurar as definições de segurança do CA EEM para o domínio

A maioria das configurações de segurança do CA EEM é criada durante a instalação do orquestrador de domínio. Uma instância do CA EEM gerencia a segurança do domínio do CA Process Automation. Portanto, essas mesmas configurações se aplicam a todos os ambientes do domínio e a todos os orquestradores em todos os ambientes. Você pode alterar as configurações somente leitura ao reinstalar o orquestrador de domínio.

Siga estas etapas:

1. Clique na guia Configuração.

   A guia Segurança é exibida.

2. Examine as configurações que foram criadas na instalação. Por exemplo, o valor de Nome do aplicativo do EEM é o valor que você deve digitar para Aplicativo nos seguintes casos:

   - Ao efetuar logon no CA EEM para criar contas de usuário.
   - Ao atribuir grupos padrão a usuários novos ou referenciados.

3. Examine o valor de Intervalo entre atualizações do cache do CA EEM.

   Esse valor expressa o intervalo (em segundos) entre as atualizações do cache do CA EEM. O cache do CA EEM contém configurações atuais de conta de usuário, grupo e diretivas do CA Process Automation. Quando o CA EEM atualiza o cache, envia ao CA Process Automation o conteúdo do cache atualizado. O valor padrão, que otimiza o desempenho do sistema, é de 1.800 segundos (30 minutos).

   - O valor padrão é adequado depois que todos os usuários estiverem configurados no CA EEM.
   - Para fazer com que essa tarefa seja realizada mais rapidamente, reduza o intervalo entre atualizações ao mínimo (60 segundos) ao testar e refinar as diretivas personalizadas. Considere a possibilidade de reduzir o intervalo em nível de ambiente para o ambiente de realização do teste.

4. Examine o valor de Domínio padrão do Active Directory, caso esteja definido.

   Esse valor é definido apenas se o CA EEM estiver configurado para usar um armazenamento de usuários externo e se Multiple Microsoft Active Directory Domains estiver selecionado. Os usuários do CA Process Automation referenciados no domínio do AD especificado aqui podem efetuar logon com um nome de usuário não adornado. Os usuários do CA Process Automation referenciados em outros domínios do AD selecionados são autenticados com seus nomes da entidade principal (isto é, *nome_do_domínio**nome_do_usuário*). A mesma diferença em convenções de nomenclatura se estende para a maneira como as identidades dos usuários são referenciadas no painel principal da guia Biblioteca.

5. Para redefinir qualquer um dos valores editáveis:

   a. Selecione o nó Domínio e clique em Bloquear.

   b. Digite um novo valor.

   c. Clique em Salvar.

   d. Selecione o nó Domínio e clique em Desbloquear.

   Se você reduzir o Intervalo entre atualizações do cache do CA EEM, considere suprimir o cache de permissões do CA Process Automation. Consulte o tópico Caches de controle de atualizações do CA EEM (na página 78).

Alterar a configuração de segurança do modo FIPS do CA EEM

Durante a instalação, a propriedade do modo FIPS do CA EEM é definida como ativada ou desativada. Essa configuração determina os algoritmos usados para criptografar os dados transferidos entre o CA EEM e o CA Process Automation. Quando o modo FIPS está ativado, os algoritmos são compatíveis com o FIPS 140-2. Quando o CA Process Automation é instalado com um CA EEM configurado com o modo FIPS definido como ativado, a configuração do certificado compatível com FIPS é exibido conforme selecionado.

É possível alterar a configuração de segurança do certificado compatível com FIPS nos seguintes níveis:

- Domain
- Ambientes
- Orquestradores

Independentemente do nível em que o certificado compatível com FIPS for alterado, ele causará impacto no domínio inteiro. O domínio tem um CA EEM. O certificado compatível com FIPS também causa impacto na configuração do modo FIPS do CA EEM e na configuração de um arquivo do iGateway.

Importante: Consulte o administrador do domínio antes de alterar qualquer configuração de segurança do CA EEM. As configurações de segurança causam um impacto abrangente.

Siga estas etapas:

1. Obtenha a senha do certificado do EEM no instalador.
2. Encerre o CA Process Automation em todos os orquestradores, exceto no orquestrador de domínio, se aplicável.
3. Efetue logon no servidor em que o orquestrador de domínio do CA Process Automation está instalado e faça o seguinte:
   a. Encerre o CA Process Automation.
   b. Interrompa o serviço do orquestrador. Por exemplo, no menu Iniciar do Windows, selecione CA, CA Process Automation 4.0, Interromper serviço do orquestrador.
4. Efetue logon no servidor em que o CA EEM está instalado e faça o seguinte:
   a. Encerre o CA EEM.
   b. Interrompa o serviço do CA iTechnology iGateway.
5. Navegue até a pasta...\CA\SharedComponents\iTechnology.
6. Altere a configuração do modo FIPS no arquivo igateway.conf.
   a. Abra o igateway.conf para edição. Por exemplo, clique com o botão direito do mouse em igateway.conf e selecione Editar no Notepad++.
   b. Localize a linha com a configuração FIPSMode. Por exemplo:

      ```
      Linha 4: <FIPSMode>off</FIPSMode>
      ```

   c. Altere o valor de desativado para ativado ou vice-versa.
   d. Salve o arquivo e feche-o.
7. Execute o utilitário do certificado do iGateway (igwCertUtil) para converter os tipos de certificado do CA EEM da seguinte maneira:
   - Se estiver alterando o modo FIPS do CA EEM para ativado (alterando uma caixa de seleção desmarcada para uma marcada), faça o seguinte:
     - Crie um tipo de certificado pem, PAM.cer e PAM.key.
     - Substitua o certificado PAM.p12 pelo tipo de certificado pem.
   - Se estiver alterando o modo FIPS do CA EEM para desativado (alterando uma caixa de seleção marcada para uma desmarcada), substitua PAM.cer e PAM.key por PAM.p12 e uma senha.

     Observação: para obter detalhes, consulte o tópico Exemplos de uso do utilitário do certificado do iGateway (na página 144).
8. Reinicie o serviço do iGateway.
9. Reinicie o CA EEM com a configuração apropriada do modo FIPS.

10. Reinicie o serviço do orquestrador no servidor com o orquestrador de domínio.
    - Interrompa o orquestrador (na página 193).
    - Inicie o orquestrador (na página 194).
11. Efetue logon no CA Process Automation e exiba a configuração de segurança do certificado compatível com FIPS e as configurações relacionadas da seguinte maneira:
    a. Efetue logon no CA Process Automation e clique na guia Configuração.
    b. Vá até o nível em que deseja implementar a alteração e bloqueie esse nível (domínio, ambiente ou orquestrador).
    c. Exiba a caixa de seleção do certificado compatível com FIPS.
    d. Se a alteração tiver sido para ativar o modo FIPS para o CA EEM, faça o seguinte:
        - Verifique se o certificado compatível com FIPS está selecionado. Se não estiver, selecione-o.
        - Digite a chave gerada no campo Chave do certificado do CA EEM.
    e. Se a alteração tiver sido para desativar o modo FIPS para o CA EEM, faça o seguinte:
        - Verifique se o certificado compatível com FIPS está desmarcado. Se não estiver, desmarque-o.
        - Digite a senha gerada no campo Senha do certificado do CA EEM.
    f. Clique em Salvar.
    g. Desbloqueie o nível, ou seja, domínio, ambiente na paleta Navegador ou orquestrador na paleta Orquestrador.
12. Reinicie o CA Process Automation em servidores com orquestradores que não sejam orquestradores de domínio.

Exemplos de uso do utilitário do certificado do iGateway

Você pode alterar a configuração de segurança do modo FIPS do CA EEM definida durante a instalação. Parte desse processo de alteração envolve usar o utilitário do certificado do iGateway (igwCertUtil). Você pode encontrar esse arquivo em ...\CA\SharedComponents\iTechnology\igwCertUtil.exe.

Observação: para obter detalhes, consulte o tópico Alterar a configuração de segurança do modo FIPS do CA EEM (na página 141).

O utilitário do certificado do iGateway inclui recursos descritos nos seguintes exemplos:

Exemplo: criar um tipo de certificado pem com arquivos PAM.cer e PAM.key

O seguinte exemplo do igwCertUtil cria um certificado pem com um arquivo .cer e .key.

```
igwCertUtil -version 4.6.0.0
-create -cert
    "<Certificate>
        <certType>pem</certType>
        <certURI>PAM.cer</certURI>
        <keyURI>PAM.key</keyURI>
        <subject>CN=PAM</subject>
    </Certificate>"
```

Exemplo: criar um tipo de certificado pem para um emissor

O seguinte exemplo do igwCertUtil cria um certificado em que o emissor nomeado forneceu o arquivo issuer.cer e issuer.key.

```
igwCertUtil -version 4.6.0.0
-create -cert
    "<Certificate>
        <certType>pem</certType>
        <certURI>PAM.cer</certURI>
        <keyURI>PAM.key</keyURI>
        <subject>CN=PAM</subject>
    </Certificate>"
-issuer
    "<Certificate>
        <certType>pem</certType>
        <certURI>issuer.cer</certURI>
        <keyURI>issuer.key</keyURI>
    </Certificate>"
```

Exemplo: copiar PAM.cer com PAM.key para PAM.p12

No exemplo a seguir, o utilitário igwCertUtil copia o certificado pem para o certificado p12 de destino. O certificado pem inclui o nome do arquivo .cer e do arquivo .key. O certificado p12 inclui a combinação de nome e senha.

```
igwCertUtil -version 4.6.0.0
-copy -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
   </Certificate>"
-target
   "<Certificate>
      <certType>p12/certType>
      <certURI>PAM.p12</certURI>
      <certPW>password</certPW>
   </Certificate>"
```

Exemplo: converter PAM.cer e PAM.key em PAM.p12 e senha

No exemplo a seguir, o utilitário igwCertUtil converte o tipo de certificado pem em um tipo de certificado p12. O utilitário converte o PAM.cer em PAM.p12 e converte o PAM.key em uma senha.

```
igwCertUtil -version 4.6.0.0
-conv -cert
   "<Certificate>
      <certType>pem</certType>
      <certURI>PAM.cer</certURI>
      <keyURI>PAM.key</keyURI>
   </Certificate>"
-target
   "<Certificate>
      <certType>p12/certType>
      <certURI>PAM.p12</certURI>
      <certPW>password</certPW>
   </Certificate>"
```

Configurar propriedades do domínio

O domínio é o elemento raiz na hierarquia do CA Process Automation. É possível editar algumas propriedades do domínio, como a frequência com que os agentes notificam o orquestrador de domínio caso eles estejam ativos. Alterar o valor dos sinais de monitoramento de 2 para 3, por exemplo, pode reduzir o tráfego de rede. A configuração que você especificar em nível de domínio pode ser herdada ou substituída em nível de ambiente.

Observação: consulte a *Referência de interface de usuário* para obter descrições dos campos.

Os administradores de conteúdo no grupo PAMAdmins podem bloquear o domínio e editar as propriedades do domínio. A permissão Domain_Admin na diretiva de domínio do CA EEM concede autorização.

Siga estas etapas:

1. Clique na guia Configuração.

   A paleta Navegador de configuração é aberta com o nó Domínio selecionado.

2. Clique na guia Propriedades.

3. Exiba os campos somente leitura, por exemplo:

   a. Exiba a entrada de URL do domínio. Essa entrada é a primeira parte do URL usado para ir até o CA Process Automation. A entrada de URL do domínio pode identificar o orquestrador de domínio ou o balanceador de carga. O URL pode indicar uma comunicação segura ou básica.

   b. Exiba a entrada de Nome do host. Essa entrada identifica o host onde o orquestrador de domínio está instalado.

   c. Exiba a entrada de Nome do orquestrador. Em nível de domínio, essa entrada é o orquestrador de domínio, por padrão.

   d. Exiba a entrada de Status. O status do domínio pode ter valores como Ativo ou Bloqueado por *ID de usuário*.

4. Com o nó Domínio selecionado, clique em Bloquear.

   Ao bloquear o domínio, somente você poderá editar as propriedades do domínio.

5. Para editar a configuração de Intervalo entre sinais de monitoramento (minutos), selecione um novo valor no controle giratório.

   A definição de um novo valor altera a frequência com que os agentes enviam um sinal de monitoramento para o orquestrador de domínio. Por padrão, os agentes enviam um sinal de monitoramento a cada 2 minutos. Essa configuração se aplica a todos os agentes no domínio, mas é possível substituir esse valor herdado para qualquer agente específico. Aumentar o valor reduz o tráfego de rede; aumentar o intervalo para cada 1 minuto permite identificar problemas no agente mais rapidamente.

6. Considere a possibilidade de deixar a configuração de Segurança do touchpoint padrão (Desativado) em vigor em nível de domínio.

   A configuração Ativado especifica que é necessário verificar e aplicar direitos de usuário nos destinos em um determinado processo. Os direitos de usuário são configurados em uma diretiva personalizada do CA EEM que usa a classe de recursos Segurança do touchpoint. É possível conceder direitos de execução para um usuário ou grupo para um determinado ambiente ou touchpoint.

   Observação: consulte Abordagem para configurar a segurança do touchpoint (na página 149).

7. Configure os destinos do Grupo de hosts de acordo com as seguintes diretrizes:

   - Desative a propriedade Fazer correspondência do destino apenas em grupos de hosts? se os padrões configurados para grupos de hosts algumas vezes fizerem correspondência com os endereços IP ou nomes de host de:

     - Hosts que instalaram agentes associados a touchpoints.
     - Hosts remotos que estão conectados a agentes associados a touchpoints do proxy.

     Observação: nesse caso, o produto desmarca a opção Pesquisar DNS ao fazer correspondência com o destino em grupos de hosts? por padrão.

   - Ative a propriedade Fazer correspondência do destino apenas em grupos de hosts? se os padrões configurados para grupos de hosts raramente fizerem correspondência com os endereços IP ou nomes de host de:

     - Hosts que instalaram agentes associados a touchpoints.
     - Hosts remotos que estão conectados a agentes associados a touchpoints do proxy.

   - Desative a propriedade Pesquisar DNS ao fazer correspondência com o destino em grupos de hosts? se os criadores de conteúdo normalmente usarem as seguintes convenções:

     - Eles usam um nome de host quando o tipo de padrão usado na configuração do Grupo de hosts for um padrão de nome de host.
     - Eles usam um endereço IP quando o tipo de padrão usado na configuração do Grupo de hosts for uma sub-rede, um intervalo de endereços IP ou uma lista de endereços IP.

   - Ative a propriedade Pesquisar DNS ao fazer correspondência com o destino em grupos de hosts? se os criadores de conteúdo estiverem cientes de que grupos de hosts fazem referência a hosts específicos de alguma forma, mas eles não sabem necessariamente como. Ativar a propriedade assegura que o operador poderá encontrar um host de destino. Por exemplo, um operador que especifica o host como um endereço IP poderá encontrar o destino quando o grupo de hosts fizer referência a ele com um padrão de nome de host.

8. Especifique os requisitos para eliminar dados de relatório que foram gerados nesse domínio. Como alternativa, é possível limpar os dados de relatórios sob demanda, em que você especifica o intervalo de datas de quando os relatórios foram gerados.
    a. Especifique se deseja limpar diariamente os dados de relatórios no campo Opção para limpar dados de relatórios. Se você selecionar Limpar dados de relatórios diariamente, especifique a hora do dia para iniciar a limpeza. Por exemplo, para iniciar a limpeza às 6:30 PM, especifique a hora militar equivalente, 18:30 no campo Hora de início da limpeza diária de dados de relatórios.
    b. Se você especificar uma programação de eliminação, indique por quantos dias os dados de relatórios devem ser mantidos antes de serem removidos. Por exemplo, uma entrada de 14 no campo Número de dias a manter os dados de relatórios especifica a limpeza de todos os dados de relatórios que existam há mais de duas semanas.
    c. Clique no botão Excluir dados de relatórios, especifique um intervalo de datas para excluir os dados de relatórios e clique em OK.
9. Para gerar relatórios de processos, marque a caixa de seleção Ativar a geração de relatório do processo. Para desativar esse recurso, desmarque a caixa de seleção Ativar a geração de relatório do processo.
10. Para gerar dados de relatório para operadores, marque a caixa de seleção Ativar a geração de relatório do operador. Para desativar esse recurso, desmarque a caixa de seleção Ativar a geração de relatório do operador.
11. Para permitir que o produto exiba logs de processo aos criadores de conteúdo no ambiente de criação, marque a caixa de seleção Ativar logs de processo. Para ocultar os logs de instância de processo em tempo de execução em nível de ambiente para o ambiente de produção, desmarque a caixa de seleção Ativar logs de processo.
12. Para automatizar a recuperação do operador, aceite o padrão para a propriedade Ativar a recuperação do operador.
13. Clique em Salvar.
14. Selecione Domínio e clique em Desbloquear.

Abordagem para configurar a segurança do touchpoint

A segurança do touchpoint é uma propriedade de nível de domínio. Por padrão, a segurança do touchpoint não é aplicada. A não aplicação herdada permite que os processos existentes sejam executados com êxito.

Observação: se você configurar a segurança do touchpoint como aplicada e não existirem diretivas de segurança do touchpoint no CA EEM, não haverá proteção.

Normalmente, hosts críticos à missão e hosts que contêm dados altamente confidenciais existem apenas em um ambiente de produção. Se você tiver particionado o domínio do CA Process Automation em um ambiente de criação e um ambiente de produção, considere estas diretrizes:

- Ambiente de criação: aceite as configurações herdadas, onde a segurança do touchpoint está desativada.
- Ambiente de produção: configure a segurança do touchpoint como Ativada nas propriedades do ambiente. Em seguida, crie uma diretiva de segurança global do touchpoint que autoriza a execução de operadores em categorias selecionadas para o grupo ou os usuários especificados por você. Especifique o ambiente como um filtro. Em seguida, especifique um filtro para cada touchpoint mapeado para um host essencial aos negócios.

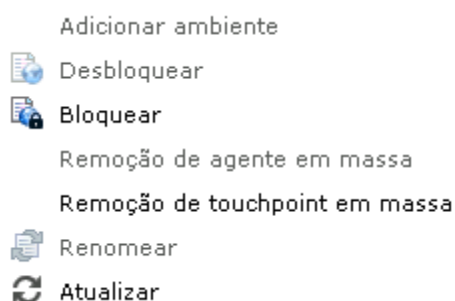
Como alternativa, você pode usar a segurança do touchpoint em um ambiente de desenvolvimento ou de teste, a fim de restringir quem pode executar processos no orquestrador. Nesse caso, você pode criar uma diretiva e listar todos os integrantes de sua equipe como Identidades. Nessa diretiva, você pode criar dois filtros -- um para o orquestrador como um touchpoint e outro para o ambiente.

Manter a hierarquia de domínio

Por padrão, todos os administradores atribuídos ao grupo PAMAdmins têm as permissões Domain_Admin. Ao usar os grupos e as diretivas personalizadas, você poderá restringir as permissões Domain_Admin para administradores selecionados.

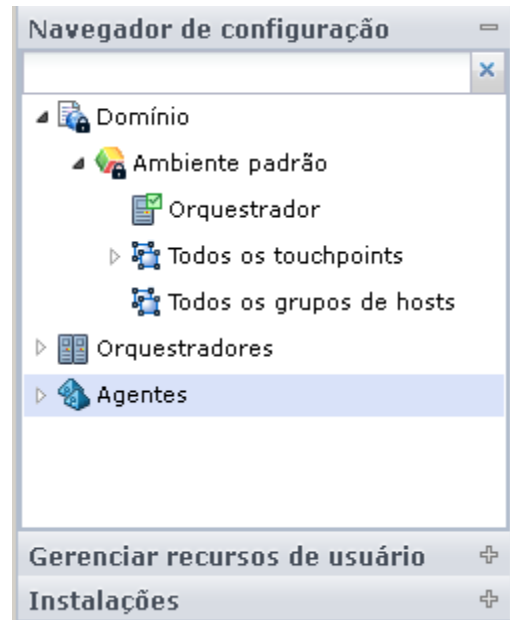
As tarefas que apenas um usuário com permissões Domain_Admin pode executar são ações que exigem o bloqueio do domínio. Consulte Bloquear e desbloquear o domínio (na página 137).

Essas tarefas alteram a hierarquia de domínio renomeando um nó, ou adicionando ou removendo nós.

Adicionar ambiente
Desbloquear
Bloquear
Remoção de agente em massa
Remoção de touchpoint em massa
Renomear
Atualizar

- Adicionar ambiente - Consulte Adicionar um ambiente ao domínio (na página 153).
- Remover ambiente - Consulte Remover um ambiente de um domínio (na página 153).
- Remoção de agente em massa - Consulte Remover agentes selecionados em massa (na página 214).
- Remoção de touchpoint em massa - Consulte Remover touchpoints vazios e não utilizados em massa (na página 231).
- Renomear o domínio - Consulte Renomear o domínio (na página 154).

Sobre a hierarquia de domínio, orquestradores e agentes

A paleta Navegador de configuração na guia Configuração contém um objeto raiz que o produto chama de domínio durante a instalação. O domínio é o elemento pai para todos os elementos configuráveis no produto.

Navegador de configuração
Domínio
Ambiente padrão
Orquestrador
Todos os touchpoints
Todos os grupos de hosts
Orquestradores
Agentes
Gerenciar recursos de usuário
Instalações

O Navegador de configuração exibe as entidades físicas e lógicas.

Físicos

Um componente *físico* é um componente instalado (um orquestrador ou um agente).

Orquestradores

Orquestrador de domínio

Imediatamente após a instalação, o orquestrador de domínio é o único componente físico.

Outros orquestradores

Os administradores podem instalar outros orquestradores na paleta Instalação.

Agentes

Os administradores podem instalar agentes na paleta Instalação.

Lógico

Uma ou mais entidades *lógicas* compõem a hierarquia de domínio, que consiste em um ou mais ambientes. Cada ambiente tem um ou mais touchpoints do orquestrador e pode ter touchpoints e grupos de hosts associados a agentes.

Domain

O domínio é o nó raiz da hierarquia de domínio. O produto tem um domínio.

Ambiente padrão

O ambiente padrão é o ambiente criado pelo programa de instalação.

Orquestrador (touchpoint)

Durante a instalação, o produto exibirá no Ambiente padrão o touchpoint do orquestrador que associa o orquestrador de domínio ao ambiente padrão. Cada orquestrador exige um touchpoint separado.

Observação: o produto associa o ambiente para um touchpoint do orquestrador agrupado ao touchpoint para esse agrupamento. Quando você usa esse touchpoint como destino de um operador, o balanceador de carga seleciona o nó de destino.

Todos os touchpoints

Durante a instalação, o nó Todos os touchpoints está vazio. Em um agente instalado, você poderá configurar um touchpoint em um ambiente selecionado. Touchpoints associam agentes a ambientes. O nó Todos os touchpoints no Ambiente padrão contém apenas touchpoints associados ao ambiente padrão. Vários touchpoints podem mapear um agente. Um único touchpoint pode ser mapeado para vários agentes.

Todos os grupos de hosts

Durante a instalação, o nó Todos os grupos de hosts está vazio. Em um agente instalado, é possível criar um grupo de hosts em um ambiente selecionado e configurar as propriedades desse grupo de hosts. A conectividade de um agente com um grupo de hosts remotos requer uma conta de usuário em cada host remoto. As contas de usuário são configuradas com as credenciais definidas nas propriedades do grupo de hosts.

Outro ambiente

Você pode adicionar um ambiente de produção separado. Cada ambiente exige pelo menos um touchpoint do orquestrador.

Outro Orquestrador (touchpoints), outro Todos os touchpoints, outro Todos os grupos de hosts no novo ambiente

Para cada orquestrador instalado, você deve criar um touchpoint em um ambiente selecionado. Os touchpoints do orquestrador são exibidos sob o nó do ambiente que você selecionar. Todos os touchpoints do agente criados são exibidos em Todos os touchpoints para o ambiente. Todos os grupos de hosts criados são exibidos em Todos os grupos de hosts para o ambiente.

Os administradores de conteúdo automatizam processos por meio da criação e da vinculação de operadores. Os operadores geralmente usam como destino (são executados em) um determinado touchpoint do orquestrador. Um operador pode usar como destino um touchpoint associado a vários agentes. Nesse caso, esse operador pode ser executado em qualquer host do agente associado.

Adicionar um ambiente ao domínio

Os administradores podem adicionar um ambiente ao domínio. Em geral, os administradores adicionam um ambiente de produção.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.

   A paleta exibe o ícone de domínio com um cadeado para indicar que está bloqueado.

2. Clique com o botão direito do mouse em Domínio e selecione Adicionar ambiente.
3. Na caixa de diálogo Adicionar novo ambiente, digite um nome para o ambiente e clique em OK.

   A paleta Navegador de configuração exibe o nome do novo ambiente com nós para adicionar Todos os touchpoints e Todos os grupos de hosts. Inicialmente, o novo ambiente não tem nenhum orquestrador.

4. Clique em Salvar.
5. Selecione Domínio e clique em Desbloquear.

Remover um ambiente do domínio

Com os direitos de administrador de domínio, você poderá excluir um ambiente do domínio. Se o ambiente for usado ativamente, execute as etapas necessárias para manter os objetos de biblioteca e os destinos de execução.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito do mouse em Domínio e, em seguida, clique em Bloquear.
3. Revise os operadores nos processos ativos que têm como destino um orquestrador ou touchpoint no ambiente de destino.
4. Reconfigure ou remova os touchpoints, touchpoints do proxy, grupos de hosts e grupos de touchpoints associados ao ambiente de destino. Por exemplo, associe touchpoints do agente a outro ambiente.

5. Mova o conteúdo da biblioteca para outro ambiente, conforme apropriado.

   Observação: os tópicos a seguir abordam como mover conteúdo:

   - Exportar uma pasta (na página 353)
   - Importar uma pasta (na página 354)

6. Remova cada orquestrador do ambiente:

   a. Coloque o orquestrador em quarentena (na página 191).

   b. Remova o orquestrador do ambiente (na página 167).

7. Clique com o botão direito do mouse no ambiente e, em seguida, selecione Excluir.

8. Clique em Sim na mensagem de confirmação.

9. Clique em Salvar.

10. Selecione Domínio e clique em Desbloquear.

Renomear o domínio

Em toda a documentação e ajuda, usamos o nome Domínio para nos referirmos ao domínio do CA Process Automation. Os administradores com as permissões Domain_Admin podem renomear o nó superior da hierarquia de domínio.

Siga estas etapas:

1. Clique na guia Configuração.
2. Selecione Domínio e clique em Bloquear.
3. Clique com o botão direito do mouse em Domínio e selecione Renomear.
4. Digite o novo nome no campo contendo o domínio.
5. Clique em Salvar.
6. Selecione Domínio e clique em Desbloquear.

Capítulo 6: Administrar os ambientes

Durante a instalação, o domínio do CA Process Automation tem um ambiente, o ambiente padrão. Os administradores definidos no grupo PAMAdmins padrão têm todos os direitos. É possível criar diretivas do CA EEM que concedam direitos de administrador específicos para diferentes usuários. Por exemplo:

- Um administrador com direitos de *Administrador de domínio* pode criar ambientes adicionais para segmentar o domínio. Normalmente, o ambiente padrão é usado para criar processos automatizados e oferecer suporte a objetos. Quando um ou mais processos estiverem prontos para serem usados no ambiente de produção existente, o administrador criará um ambiente no CA Process Automation e dará um nome ao ambiente de produção. Outros exemplos incluem a segmentação geográfica, a segmentação do ciclo de vida e o armazenamento temporário. Essas tarefas são abordadas nesse capítulo.
- Um administrador com direitos de *Administrador de conteúdo do ambiente* pode adicionar touchpoints, grupos de hosts, criar grupos de touchpoints e remover touchpoints não utilizados em massa. Eles também podem criar novos objetos, incluindo processos e programações. Consulte os capítulos subsequentes para obter detalhes sobre touchpoints e grupos de hosts. Consulte o *Guia do Criador de Conteúdo* para obter detalhes sobre como usar as guias Biblioteca e Criador para criação e desenvolvimento de conteúdo.
- Um administrador com direitos de *Administrador de configuração do ambiente* pode configurar o conteúdo de um ambiente selecionado. Os administradores podem aceitar ou substituir as configurações herdadas. A configuração do conteúdo de um ambiente pode incluir editar as configurações de segurança, definir propriedades do ambiente, ativar ou desativar categorias de operador e definir a herança dos disparadores.

Esta seção contém os seguintes tópicos:

Configurar o conteúdo de um ambiente

Quando você seleciona um ambiente no Navegador de configuração, as seguintes guias são exibidas em Conteúdo de "<nome do ambiente>":

Conteúdo de "Ambiente padrão"
Segurança | Admissão auto... | Propriedades | Módulos | Disparadores | Trilhas de audit...

- Segurança

  Consulte Exibir ou redefinir as configurações de segurança de um ambiente selecionado (na página 156).

- Admissão automática

  Consulte Adicionar touchpoints para agentes em massa (na página 228).

- Propriedades

  Consulte Configurar propriedades do ambiente (na página 157).

- Módulos

  Consulte Ativar uma categoria do operador e substituir configurações herdadas (na página 161).

- Gatilhos

  Consulte Especificar configurações do disparador de um ambiente (na página 162).

- Trilhas de auditoria

  Consulte Exibir a trilha de auditoria de um ambiente (na página 336).

Exibir ou redefinir as configurações de segurança de um ambiente selecionado

A maioria das configurações da guia Segurança é criada durante a instalação ou atualização do orquestrador de domínio. Você pode alterar essas configurações somente leitura apenas reinstalando o orquestrador de domínio.

Cada ambiente herda as configurações estabelecidas durante a instalação do orquestrador de domínio. Se você desmarcar a caixa de seleção Herdar, poderá atualizar o Intervalo entre atualizações do cache do CA EEM (em segundos). Ao reduzir o intervalo de atualização, o CA Process Automation reflete as alterações feitas no CA EEM mais rapidamente.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a opção Domínio na paleta Navegador de configuração e, em seguida, selecione o ambiente de destino.

   A guia Segurança é exibida.

3. Examine as configurações de segurança que foram estabelecidas durante o processo de instalação.

4. (Opcional) Atualize o valor de Intervalo entre atualizações do cache do CA EEM.
   a. Clique em Bloquear.
   b. Desmarque a caixa de seleção Herdar.
   c. Atualize o valor.
   d. Clique em Salvar.
   e. Selecione o ambiente e clique em Desbloquear.

   Observação: se você reduzir o Intervalo entre atualizações do cache do CA EEM, considere suprimir o cache de permissões do CA Process Automation. Consulte o tópico Caches de controle de atualizações do CA EEM (na página 78).

Configurar propriedades do ambiente

Configure as propriedades de um ambiente selecionado na guia Configuração. É necessário ter direitos de administrador de configuração do ambiente para configurar propriedades do ambiente ou substituir as configurações em um nível que possa herdar do ambiente.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o nó Domínio, clique com o botão direito do mouse no ambiente apropriado e clique em Bloquear.
3. Clique na guia Propriedades e, em seguida, exiba ou atualize as propriedades, conforme apropriado.

   Recuperação automática de operadores

   Especifica onde recuperar automaticamente. A recuperação se aplica aos operadores que falham com um SYSTEM_ERROR e que possuem processos recuperáveis nos estados BLOQUEADO, EM EXECUÇÃO ou AGUARDANDO. Selecione Verdadeiro para iniciar a recuperação quando o orquestrador ou o agente inativo ficar ativo. Recuperação redefine os operadores que estavam em SYSTEM_ERROR e reinicia os processos. Os operadores redefinidos em um processo retomado começam a ser executados nos destinos associados. Os destinos dos operadores podem ser orquestradores, touchpoints, hosts conectados a touchpoints do proxy ou hosts de um grupo de hosts.

   Valores: esta propriedade possui os seguintes valores:

   - **Selecionado** - Automatiza a recuperação.
   - **Desmarcado** - Impede a recuperação automática.

   Padrão: Selecionado.

Segurança do touchpoint

Especifica se é necessário herdar o valor configurado nas propriedades do domínio ou definir o valor no nível de ambiente.

Valores: esta propriedade possui os seguintes valores:

- **Herdar do domínio** - Usar o valor configurado para este campo nas propriedades do domínio.
- **Ativado** - Aplicar diretivas de segurança do touchpoint para esse destino e permitir acesso somente se o usuário tiver recebido essa permissão.
- **Desativado** - Não verificar se o usuário que está executando o processo tem direitos de execução no destino atual.

Padrão: Herdar do domínio.

Fazer correspondência do destino apenas em grupos de hosts?

Especifica o escopo de pesquisa para o destino de um operador quando a entrada do campo Destino for um endereço IP ou um nome de host (FQDN). A execução do operador no destino pode prosseguir somente quando o destino for conhecido no CA Process Automation. Selecione Desativado para permitir a pesquisa mais ampla. Selecione Ativado aqui e Desativado no próximo campo para a pesquisa mais restrita.

Observação: a pesquisa de DNS de um nome de host especificado localiza endereços IP associados; a pesquisa de DNS do endereço IP localiza nomes de host associados.

Valores: esta propriedade possui os seguintes valores:

- **Herdar do domínio** - Usar o valor configurado para este campo nas propriedades do domínio.
- **Ativado** - O escopo da pesquisa depende se o campo Pesquisar DNS ao fazer correspondência com o destino em grupos de hosts está ativado ou desativado.

  Se uma pesquisa de DNS estiver desativada, pesquisa: referência de grupo de hosts para um host remoto (exatamente)

  Se uma pesquisa de DNS estiver ativada, pesquisa: referência de grupo de hosts para um host remoto (exatamente ou resultado de pesquisa de DNS)
- **Desativado** - Pesquisar os componentes do domínio na seguinte ordem:

  Touchpoint (exatamente ou resultado de pesquisa de DNS)

  Orquestrador (exatamente ou resultado de pesquisa de DNS)

  Agente (exatamente ou resultado de pesquisa de DNS)

  Mapeamento de touchpoint do proxy para um host remoto (exatamente ou resultado de pesquisa de DNS)

  Referência de grupo de hosts para um host remoto (exatamente ou resultado de pesquisa de DNS)

Padrão: Herdar do domínio.

Pesquisar DNS ao fazer correspondência com o destino em grupos de hosts?

Observação: esse campo é ativado quando Fazer correspondência do destino apenas em grupos de hosts estiver definido como Ativado.

Especifica se é necessário limitar a pesquisa pelas referências de grupo de hosts para o tipo de entrada. Por exemplo: quando o tipo de entrada do campo Destino for um FQDN, pesquisa apenas padrões de nomes de hosts. Quando o tipo de entrada do campo Destino for um endereço IP, pesquisa apenas sub-redes. Quando uma pesquisa de DNS for incluída, a pesquisa também poderá aceitar uma referência de grupo de hosts para o outro tipo, como resolvido por uma pesquisa de DNS.

Valores: esta propriedade possui os seguintes valores:

- **Herdar do domínio** - Usar o valor configurado para este campo nas propriedades do domínio.
- **Ativado** - Pesquisar todas as referências de grupo de hosts. As referências de grupo de hosts para nomes de host são padrões (expressões regulares) que podem incluir o nome de host especificado. As referências de grupo de hosts para endereços IP são sub-redes do endereço IP que são expressas em notação CIDR que pode incluir o endereço IP especificado. Estender a pesquisa a todas as referências de grupo de hosts. Permite que a pesquisa encontre uma correspondência exata ou uma correspondência para o resultado de pesquisa de DNS.
- **Desativado** - Restringir a pesquisa às referências de grupo de hosts que incluem uma correspondência exata para a entrada do campo Destino.

Padrão: Herdar do domínio.

4. Clique em Salvar.
5. Selecione o ambiente e clique em Desbloquear.

   As atualizações da propriedade de ambiente estão ativas.

Ativar uma categoria do operador e substituir configurações herdadas

As configurações de categoria de operadores são exibidas em um ambiente como Herdar do domínio por padrão. Quando as configurações de categoria do operador são definidas no nível do domínio, um administrador pode aceitar as configurações herdadas. Como alternativa, um administrador com direitos de administrador de configuração do ambiente pode ativar qualquer categoria de operador e substituir as configurações herdadas no nível do ambiente.

Para examinar as configurações de qualquer categoria de operador, é necessário ativar a categoria.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o domínio, selecione um ambiente e clique em Bloquear.
3. Clique na guia Módulos.
4. Para exibir as configurações de qualquer categoria de operador, clique em Herdar do domínio e selecione Ativar na lista suspensa.
5. Clique com o botão direito do mouse na categoria do operador e selecione Editar.

   As configurações atuais são exibidas.
6. Opcionalmente, defina as configurações de um ou mais campos.

   Observação: consulte Configurando categorias do operador (na página 270) para obter detalhes de nível de campo.
7. Clique em Salvar.
8. Clique em Fechar.
9. Clique com o botão direito do mouse no ambiente e selecione Desbloquear.

Especificar configurações do disparador de um ambiente

As configurações do disparador são desativadas no nível de ambiente por padrão. Se a configuração do disparador tiver sido definida no nível de domínio, você poderá especificar se deseja herdar essas configurações. Como alternativa, é possível ativar um disparador e, em seguida, substituir as configurações no nível de domínio. Se necessário, você pode desativar um disparador que está ativado ou definido para herdar valores.

Siga estas etapas:

1. Clique na guia Configuração.
2. Revise as configurações no nível de domínio para o disparador:
   a. Clique em Domínio
   b. Clique na guia Disparadores.
   c. Clique duas vezes em um disparador.
   d. Determine se o disparador foi configurado e, em caso afirmativo, se deseja aceitar as configurações para um determinado ambiente.
3. Selecione um ambiente e clique em Bloquear.
4. Clique na guia Disparadores.
5. Selecione um disparador.
6. Selecione um novo valor na lista suspensa.

   Herdar do domínio

   Especifica se as definições configuradas no nível de domínio serão usadas no ambiente selecionado.

   Desabilitado

   Especifica que esse disparador não será usado nesse ambiente.

   Ativado

   Especifica que esse disparador é para usar as configurações definidas para esse ambiente.

7. Se você selecionar Ativado, clique com o botão direito do mouse no disparador e selecione Editar. Edite as configurações usando os procedimentos a seguir como um guia:
   - Configurar as propriedades do disparador de arquivo no nível do domínio (na página 319).
   - Configurar propriedades do disparador de email no nível do domínio (na página 320).
   - Configurar propriedades do disparador do SNMP no nível do domínio (na página 323).

- Configurar propriedades do disparador do Catalyst no nível do domínio (na página 316).

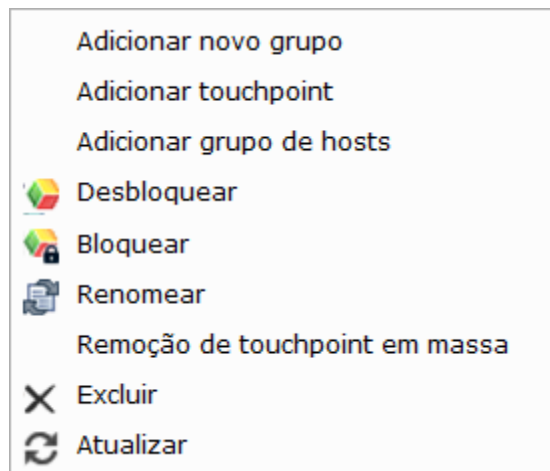
8. Clique em Salvar.
9. Clique em Fechar.
10. Selecione o ambiente atualizado e clique em Desbloquear.

Atualizar uma hierarquia de ambiente

A hierarquia de domínio é composto de um ou mais ambientes, onde cada ambiente tem ao menos um orquestrador e um ou mais touchpoints que associam o ambiente a um agente. Quando um operador em um processo em andamento tem como destino um touchpoint, esse operador é executado no agente ou orquestrador associado ao touchpoint. Quando um operador tem um grupo de touchpoints como destino, ele é executado em todos os orquestradores e agentes associados.

Para oferecer suporte à execução de operadores em hosts remotos, que são hosts sem agente, um ambiente pode incluir touchpoints do proxy e grupos de hosts. Um touchpoint do proxy associa um host remoto a um agente; um grupo de hosts associa muitos hosts remotos a um agente. Em ambos os casos, o host do agente se conecta ao host remoto com uma conexão SSH confiável.

Um administrador com as permissões Environment_Configuration_Admin (Administrador de configuração) pode atualizar a hierarquia de um ambiente selecionado. As opções de menu de clique com o botão direito do mouse para um ambiente são as seguintes:

Adicionar novo grupo
Adicionar touchpoint
Adicionar grupo de hosts
Desbloquear
Bloquear
Renomear
Remoção de touchpoint em massa
Excluir
Atualizar

Os links para tópicos das opções do menu Ambiente seguem abaixo:

- Adicionar novo grupo

  Consulte Agrupar touchpoints em um ambiente (na página 233).

- Adicionar touchpoint

  Consulte Adicionar um touchpoint e criar uma associação (na página 226) e outros detalhes nos capítulos "Administrar touchpoints" e "Administrar touchpoints do proxy".

  Consulte também Adicionar um orquestrador a um ambiente (na página 166).

- Adicionar grupo de hosts

  Consulte Criar um grupo de hosts (na página 250) e outros detalhes no capítulo Administrar grupos de hosts.

- Renomear

  Consulte Renomear um ambiente (na página 165).

- Remoção do Touchpoint em massa

  Consulte Remover touchpoints vazios e não utilizados em massa (na página 231).

- Excluir - Pode ser usado para remover qualquer objeto lógico adicionado pelo usuário da hierarquia de domínio, ou seja:
  - Qualquer ambiente.
  - Qualquer touchpoint do orquestrador.

    Consulte o tópico Excluir um touchpoint do orquestrador (na página 167).
  - Qualquer touchpoint do agente.
  - Qualquer grupo de touchpoints.
  - Qualquer grupo de hosts.

Renomear um ambiente

Os administradores com direitos Environment_Configuration_Admin (Administrador de configuração) podem renomear um ambiente.

Siga estas etapas:

1. Clique na guia Configuração.

   A paleta do navegador de configuração é aberta.

2. Clique com o botão direito do mouse em Domínio e clique em Bloquear.
3. Clique com o botão direito do mouse no ambiente e clique em Bloquear.
4. Clique com o botão direito do mouse no ambiente e selecione Renomear.
5. Insira o novo nome do ambiente.
6. Clique em Salvar.
7. Clique com o botão direito do mouse em Domínio e clique em Desbloquear.

Adicionar um Orquestrador a um ambiente

Durante a instalação inicial do CA Process Automation, o Orquestrador de domínio é instalado no Ambiente padrão. O ambiente padrão é normalmente usado para criação e teste. Em geral, os administradores criam um ambiente separado para produção.

Cada ambiente deve ter ao menos um orquestrador, mas qualquer ambiente pode ter vários orquestradores. Cada novo orquestrador envolve uma instalação separada. Após instalar um orquestrador separado, adicione-o a um ambiente.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito do mouse no ambiente a ser configurado e clique em Bloquear.
3. Clique com o botão direito do mouse no ambiente novamente e clique em Adicionar touchpoint.

   A caixa de diálogo Adicionar Touchpoint é aberta.
4. Ao lado do Nome de Touchpoint, digite um nome para o novo Orquestrador.
5. Ao lado de Selecionar agente/orquestrador, clique em Orquestrador.

   A opção Orquestrador não estará disponível se todos os orquestradores no domínio já estiverem associados a touchpoints existentes.
6. Na lista de orquestradores disponíveis, selecione o orquestrador que deseja associar ao novo touchpoint.
7. Clique em Salvar para adicionar o novo touchpoint ao ambiente.
8. Selecione a paleta Navegador, clique com o botão direito do mouse no ambiente e clique em Desbloquear.

   A caixa de diálogo dados não salvos avisa para salvar as alterações.
9. Clique em Sim.

   Observação: também é possível salvar usando Salvar na parte superior da tela ou por meio do menu Arquivo sem desbloqueá-lo.

Mais informações:

Adicionar um Touchpoint a um Orquestrador (na página 177)

Excluir um touchpoint do orquestrador

Um touchpoint do orquestrador é uma entidade lógica que associa um orquestrador selecionado, ou seu balanceador de carga, a um ambiente específico. Excluir um touchpoint do orquestrador remove a associação, mas não afeta o ambiente ou o orquestrador. No entanto, um orquestrador físico sem touchpoint não pode ser acessado. Ele não pode aceitar solicitações do operador nem atualizações para sua biblioteca.

Você pode excluir um touchpoint do orquestrador como preparação para a criação de um novo touchpoint para esse orquestrador. Você pode excluir um touchpoint do orquestrador como preparação para a desativação desse orquestrador.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o nó do domínio e o nó do ambiente com o orquestrador a ser removido.
3. Clique com o botão direito do mouse no domínio e clique em Bloquear.
4. Clique com o botão direito do mouse no ambiente que contém o orquestrador que você deseja excluir e clique em Bloquear.
5. Clique com o botão direito no Orquestrador que você deseja excluir e selecione Excluir.
6. Clique em OK para confirmar a exclusão do Orquestrador.
7. Clique com o botão direito do mouse no ambiente e clique em Desbloquear.
8. Clique com o botão direito em Domínio e clique em Desbloquear.

   O touchpoint do orquestrador é excluído.

Capítulo 7: Administrar Orquestradores

É possível instalar quantos orquestradores forem necessários. A primeira instalação cria o orquestrador de domínio. Depois que o orquestrador de domínio está em execução, é possível instalar outros orquestradores por meio da paleta de instalação na guia Configuração.

Os orquestradores são os "mecanismos" do CA Process Automation; eles processam o conteúdo que é criado com o CA Process Automation. Todos os processos são executados em orquestradores, os quais gerenciam e executam os objetos de automação. Os orquestradores direcionam os agentes para que executem as ações necessárias como parte do processo.

Esta seção contém os seguintes tópicos:

Sobre Orquestradores

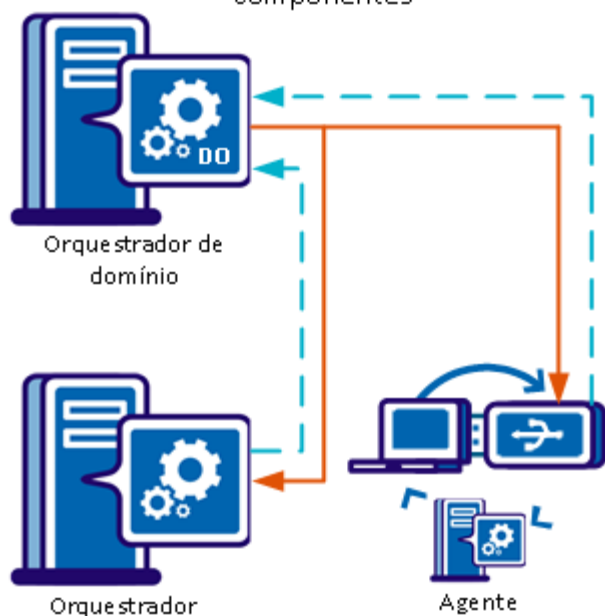
O orquestrador de domínio mantém a configuração e o status de todos os componentes no domínio. É possível fazer upload das atualizações de orquestradores ou agentes para o orquestrador de domínio. O orquestrador de domínio envia as atualizações que você carregar para todos os orquestradores ou agentes. Todos os orquestradores e agentes no domínio enviam seus status para o orquestrador de domínio regularmente.

O orquestrador de domínio faz a manutenção dos componentes

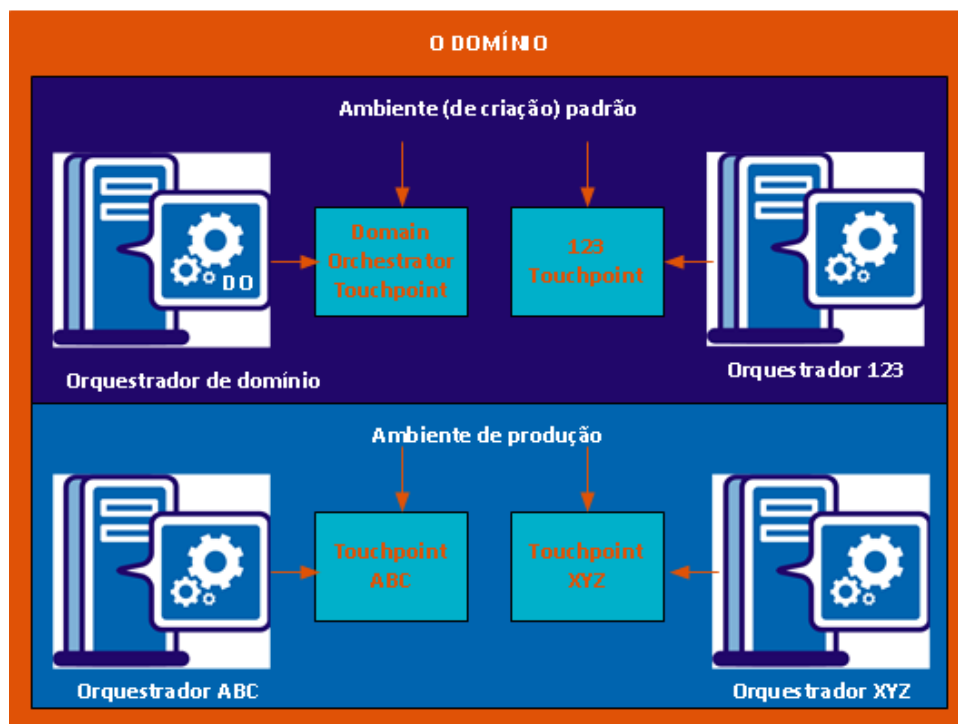
DO

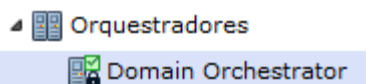
Orquestrador de domínio

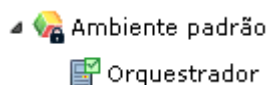
Orquestrador

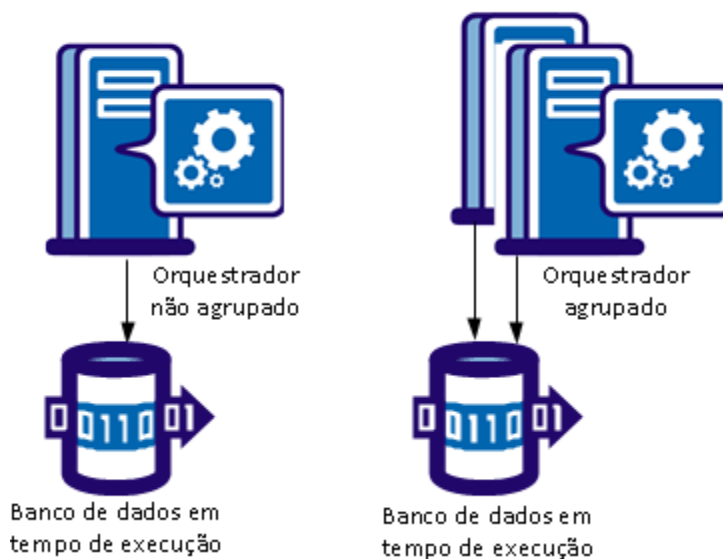
Agente

Para adicionar um orquestrador a um ambiente, configure um touchpoint para o orquestrador selecionado no ambiente que você especificar. Cada orquestrador participa somente de um ambiente do CA Process Automation. Cada orquestrador está associado a um touchpoint. Quando um operador deve ser executado em um touchpoint do orquestrador, o campo Destino é deixado em branco. Um campo Destino em branco significa executar o operador no orquestrador em que o processo foi iniciado.

Um touchpoint de orquestrador associa o orquestrador a um ambiente

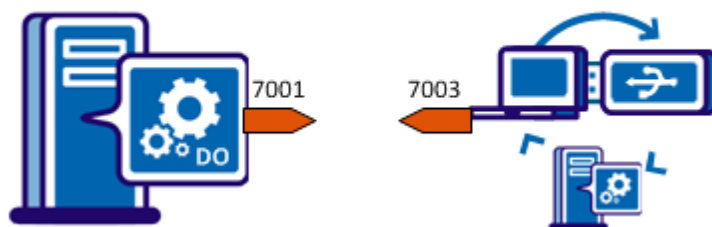
O DOMÍNIO
Ambiente (de criação) padrão
Domain Orchestrator Touchpoint
123 Touchpoint
DO
Orquestrador de domínio
Orquestrador 123
Ambiente de produção
Touchpoint ABC
Touchpoint XYZ
Orquestrador ABC
Orquestrador XYZ

É possível definir configurações específicas do host e exibir informações físicas de um orquestrador no nó Orquestradores.

Orquestradores
Domain Orchestrator

Defina configurações específicas do touchpoint para o mesmo orquestrador no nó do ambiente. É possível exibir informações lógicas sobre um orquestrador no respectivo ambiente.

Ambiente padrão
Orquestrador

Os orquestradores podem ser *agrupados* (com vários nós) para alta disponibilidade e escalabilidade ou *não agrupados* (com um único nó). Um orquestrador agrupado atua como um único orquestrador. Por exemplo, enquanto cada orquestrador não agrupado possui seu próprio banco de dados de tempo de execução, os orquestradores em um nó agrupado compartilham um banco de dados de tempo de execução.

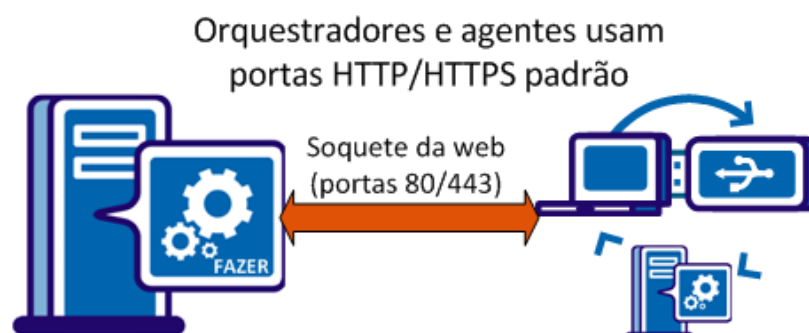
Orquestradores agrupados e não agrupados têm comportamento semelhante

Um processo que é executado em um orquestrador pode executar um subprocesso em um orquestrador separado. Um agente pode executar etapas de um processo (como a execução de um script). Os orquestradores e agentes usam um par de portas de comunicação.

Com a comunicação obsoleta, a porta padrão para os orquestradores é a 7001; a porta padrão para os agentes é a 7003. As portas 7001 e 7003 são bidirecionais, isto é, essas portas enviam e recebem dados.

Orchestrators and Agents Have Default Ports

Com a comunicação simplificada, os agentes iniciam uma conexão de soquete da web persistente que o agente e o orquestrador usam para comunicação.

Orquestradores e agentes usam portas HTTP/HTTPS padrão

Soquete da web (portas 80/443)

FAZER

Quando o orquestrador solicita que um agente conclua uma etapa, o agente retorna os resultados para o orquestrador. Em uma instalação agrupada, um nó do orquestrador envia uma solicitação para um agente. O agente envia o resultado para qualquer nó do orquestrador solicitante. Um dos nós do agrupamento captura o resultado do agente em uma fila compartilhada.

Configurar o conteúdo de um touchpoint do orquestrador

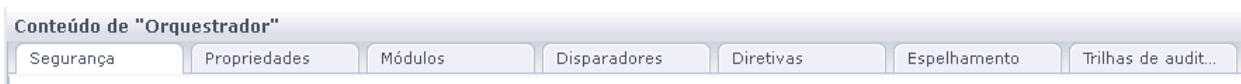
Para configurar um touchpoint do orquestrador, selecione o orquestrador em um nó Ambiente. Tudo, menos uma das configurações é apenas para exibição.

Para definir configurações que pertencem ao host do orquestrador, selecione o orquestrador no nó Orquestradores.

Observação: para obter detalhes da configuração, consulte Configurar o conteúdo de um host do orquestrador (na página 180).

As guias de conteúdo do orquestrador selecionado seguem abaixo:

Conteúdo de "Orquestrador"

Segurança | Propriedades | Módulos | Disparadores | Diretivas | Espelhamento | Trilhas de audit...

O único campo configurável nesse conjunto de guias é para a segurança do touchpoint. Na guia Propriedades, defina Segurança do Touchpoint como Verdadeiro somente depois de ter configurado uma diretiva de segurança do touchpoint.

Os tópicos das guias Orquestrador seguem abaixo:

- Segurança - as configurações de segurança não se aplicam ao touchpoint do orquestrador. Os campos são somente leitura na exibição Touchpoint de orquestrador.
- Propriedades - é possível configurar as propriedades do touchpoint do orquestrador (na página 174).
- Módulos - não é possível configurar as categorias de operadores a partir de um touchpoint de orquestrador. É possível editar as configurações selecionando o host do orquestrador.
- Disparadores - os disparadores não são configuráveis em um touchpoint de orquestrador. É possível editar as configurações selecionando o host do orquestrador.
- Diretivas - as diretivas não são configuráveis em um touchpoint de orquestrador. É possível editar as configurações selecionando o host do orquestrador.
- Espelhamento - o espelhamento não é configurável em um touchpoint de orquestrador. É possível editar a configuração de espelhamento selecionando o host do orquestrador correspondente.
- Trilhas de auditoria - as ações da trilha de auditoria não se aplicam aos touchpoints de orquestrador. Você pode exibir as ações auditadas no host do orquestrador correspondente.

Configurar as propriedades do touchpoint do orquestrador

O painel Propriedades do touchpoint do orquestrador fornece informações sobre o touchpoint associado ao orquestrador. Você pode exibir as informações de status e alterar a configuração de Segurança do touchpoint para esse touchpoint de orquestrador.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o Domínio e o ambiente com o touchpoint de orquestrador.
3. Selecione o touchpoint de orquestrador para configurar e clique em Bloquear.
4. Clique na guia Propriedades.
5. (Opcional) Defina a configuração de Segurança do touchpoint. Especifique se deseja herdar a configuração ou definir o valor em nível de orquestrador. Quando ativados, os processos usam as diretivas de Segurança do touchpoint para autorizar os usuários a executar operadores em um processo.

6. Defina as configurações padrão para indicar como os operadores processam um endereço IP ou nome do host no campo Destino ou quando são referenciados por um conjunto de dados.

   a. A seleção da lista suspensa Fazer correspondência do destino apenas em grupos de hosts? especifica o escopo de pesquisa para o destino de um operador quando a entrada do campo Destino for um endereço IP ou um nome de host (FQDN). A execução do operador no destino pode prosseguir somente quando o destino for conhecido no CA Process Automation.

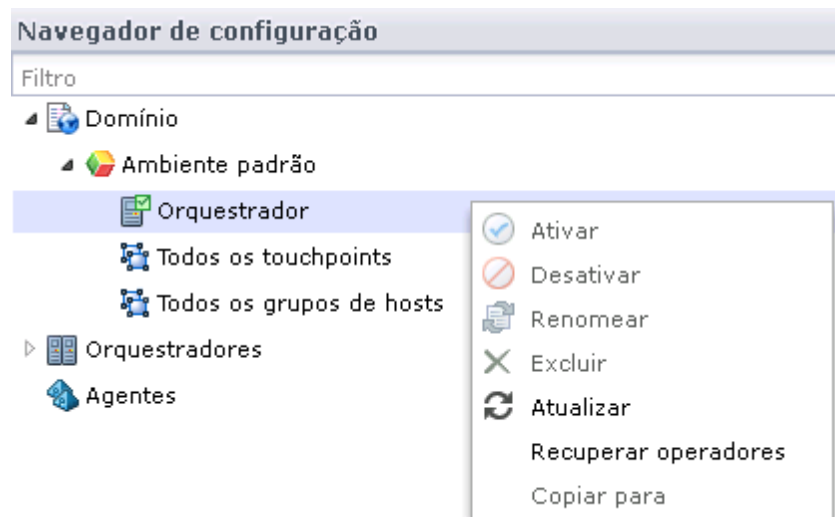
      - Selecione Desativado para permitir a pesquisa mais ampla.
      - Selecione Ativado aqui e Desativado no próximo campo para a pesquisa mais restrita.

   b. Quando a lista suspensa Pesquisar DNS ao fazer correspondência com o destino em grupos de hosts? estiver ativada, especifique se deseja limitar a pesquisa por meio de referências de grupo de hosts para o tipo de entrada.

      - Selecione Ativado para pesquisar todas as referências de grupo de hosts.
      - Selecione Desativado para restringir a pesquisa a referências de grupo de hosts que incluem uma correspondência exata com a entrada do campo Destino.

7. Clique em Salvar.
8. Selecione o orquestrador e clique em Desbloquear.
9. Exiba as propriedades informativas. Para obter mais informações, consulte as dicas de ferramenta.

Atualizar a hierarquia de um touchpoint do orquestrador

Quando você seleciona um orquestrador em Domínio/ambiente, os detalhes exibidos são relevantes para o touchpoint mapeado para esse orquestrador.

Observe o seguinte:

- Ativar - clique com o botão direito em um touchpoint do orquestrador que está desativado e selecione Ativar.
- Desativar

  Consulte Desativar um touchpoint de orquestrador (na página 179).
- Renomear - especifique um novo nome para o touchpoint do orquestrador.
- Excluir - clique com o botão direito do mouse em um touchpoint de orquestrador e selecione Excluir. Apenas o touchpoint é excluído.
- Recuperar operadores

  Consulte Recuperar operadores no orquestrador de destino (na página 177).
- Copiar para

  Consulte Criar um grupo de touchpoints com touchpoints selecionados (na página 235)

Adicionar um Touchpoint a um Orquestrador

Quando você adicionar um orquestrador autônomo a um ambiente, adicione um touchpoint ao ambiente e mapeie-o para esse orquestrador. Cada orquestrador deve ser associado ao seu próprio touchpoint.

Quando você adiciona nós para criar um orquestrador agrupado, o balanceador de carga usa o touchpoint definido para o primeiro nó. O balanceador de carga determina qual nó manipula uma solicitação que se destina ao touchpoint.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito do mouse no ambiente ao qual deseja adicionar um touchpoint e clique em Bloquear.
3. Expanda o nó Orquestradores.
4. Clique com o botão direito do mouse no orquestrador de destino, selecione Configurar touchpoint em e clique no nome do ambiente que você bloqueou.
5. Na caixa de diálogo Adicionar touchpoint de orquestrador, digite um nome para o novo touchpoint e clique em Adicionar.
6. Clique com o botão direito do mouse no ambiente ao qual você adicionou o touchpoint e selecione Desbloquear.

   A caixa de diálogo Dados não salvos avisa para salvar as alterações.
7. Clique em Sim.

   Um novo touchpoint do orquestrador é adicionado ao ambiente selecionado.

Mais informações:

Adicionar um Orquestrador a um ambiente (na página 166)

Recuperar operadores no Orquestrador de destino

A recuperação manual está sempre ativada. É possível chamar Recuperar operadores se o nível de destino da Recuperação automática de operadores estiver definido como Verdadeiro, Falso ou Herdar do ambiente. A recuperação do operador é apropriada quando um processo estiver em um estado BLOQUEADO, EM EXECUÇÃO ou AGUARDANDO e um operador no processo tiver falhado com um erro de sistema. A recuperação do operador redefine o operador e retoma o processo.

É possível chamar a recuperação dos operadores na guia Configuração quando:

- O orquestrador anteriormente inativo se torna ativo. Um orquestrador ativo é exibido em verde.
- O orquestrador de destino é ativado.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a opção Domínio e um ambiente em que um orquestrador possua um ou mais processos que estejam definidos como recuperáveis.
3. Clique com o botão direito do mouse no orquestrador e selecione Atualizar.
4. Clique com o botão direito do mouse no orquestrador e selecione Recuperar operadores.

   A recuperação do operador é iniciada.

Desativar um touchpoint de orquestrador

Desative um touchpoint de orquestrador para impedir que os processos sejam executados nele. A desativação de um touchpoint de orquestrador não afeta a biblioteca do orquestrador. Ou seja, os criadores podem selecionar um orquestrador com um touchpoint desativado na guia Biblioteca e definir os objetos de automação.

Você deve desativar um touchpoint de orquestrador quando os objetos externos afetados não estiverem disponíveis. Considere o exemplo de processos que lidam com o Service Desk ou com um banco de dados externo. Às vezes, esses componentes estarão desligados para manutenção. Você pode impedir a execução de processos que interagem com componentes que estão temporariamente indisponíveis. Quando os componentes externos se tornarem disponíveis, você poderá ativar o touchpoint de orquestrador. Em seguida, os processos programados que usam esses componentes externos poderão começar a ser executados novamente.

É possível desativar o touchpoint do orquestrador que você selecionar na hierarquia de domínio.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o nó do domínio. Expanda o nó do ambiente com o touchpoint de orquestrador a ser desativado.
3. Selecione um ambiente e clique em Bloquear.
4. Selecione o touchpoint de orquestrador e clique em Bloquear.
5. Clique com o botão direito do mouse no touchpoint do orquestrador e selecione Desativar.
6. Clique em Desbloquear.
7. Selecione o ambiente bloqueado e clique em Desbloquear.

Mais informações:

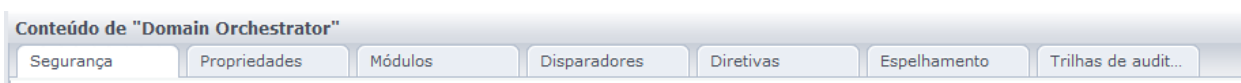
Colocar um Orquestrador em quarentena (na página 191)

Configurar o conteúdo de um host do orquestrador

Os detalhes da configuração que são exclusivos aos orquestradores e não são herdados incluem diretivas e espelhamento, em que ambos possuem valores padrão para todos os campos. O espelhamento se aplica aos orquestradores, exceto ao orquestrador de domínio. As configurações para segurança, propriedades, módulos e disparadores são herdadas por padrão. As configurações que você define para um host do orquestrador são diferentes das definidas no touchpoint do orquestrador.

Veja a seguir as guias do menu Host do orquestrador:

Conteúdo de "Domain Orchestrator"

Segurança | Propriedades | Módulos | Disparadores | Diretivas | Espelhamento | Trilhas de audit...

- Segurança

  Consulte Exibir as configurações de segurança do orquestrador (na página 181).

- Propriedades

  Consulte Configurar as propriedades do touchpoint de orquestrador (na página 174).

- Módulos

  Consulte Substituir configurações de categoria de operador herdadas do ambiente (na página 185).

- Gatilhos

  Consulte Ativar disparadores para um orquestrador (na página 186).

- Políticas

  Consulte Configurar diretivas do orquestrador (na página 187).

- Espelhamento

  Consulte Configurar espelhamento do orquestrador (na página 189).

- Trilhas de auditoria

  Consulte Exibir a trilha de auditoria de um orquestrador (na página 338).

Exibir as configurações de segurança do orquestrador

A maioria das configurações da guia Segurança é criada durante o processo de instalação do orquestrador de domínio. Não é possível alterar essas configurações na interface do usuário. Você pode alterar essas configurações reinstalando o orquestrador de domínio.

A caixa de seleção Herdar se aplica somente ao Intervalo entre atualizações do cache do CA EEM (em segundos). Você pode reduzir o intervalo entre atualizações quando desejar que o CA Process Automation receba alterações que você fizer no CA EEM com mais rapidez.

Siga estas etapas:

1. Clique na guia Configuração.
2. Na paleta Navegador de configuração, expanda Orquestradores.
3. Selecione um orquestrador. Você pode exibir as configurações de segurança na guia Segurança.
4. Para atualizar as configurações:
    a. Clique em Bloquear.
    b. Desmarque a caixa de seleção Herdar.
    c. Atualize o Intervalo entre atualizações do cache do CA EEM (em segundos).
    d. Clique em Salvar.
    e. Clique em Desbloquear.

Configurar propriedades do host do orquestrador

Você pode configurar as propriedades do host de um orquestrador selecionado e exibir informações somente leitura.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o nó Orquestradores.
3. Selecione o orquestrador a ser configurado e clique em Bloquear.

4. Clique na guia Propriedades e exiba as configurações de propriedades do orquestrador somente leitura:
   - É domínio
   - Nome do host
   - Nome do orquestrador
   - Status
5. Defina os seguintes campos:

   Recuperação automática de operadores

   Especifica onde recuperar automaticamente. A recuperação se aplica aos operadores que falham com um SYSTEM_ERROR e cujos processos recuperáveis estão nos estados BLOQUEADO, EM EXECUÇÃO ou AGUARDANDO quando a recuperação é disparada. Se a recuperação for definida para automática, cada orquestrador no ambiente iniciará automaticamente a recuperação quando o orquestrador tornar-se ativo novamente. A recuperação começa com os processos afetados e seus operadores afetados começam a ser executados nesse orquestrador.

   Valores: esta propriedade possui os seguintes valores:
   - **Herdar do ambiente** - Usar o valor configurado para este campo nas propriedades do ambiente.
   - **Verdadeiro** - Automatiza a recuperação.
   - **Falso** - Impede a recuperação automática.

   Padrão: Herdar do ambiente.

Fazer correspondência do destino apenas em grupos de hosts?

Especifica o escopo de pesquisa para o destino de um operador quando a entrada do campo Destino for um endereço IP ou um nome de host (FQDN). A execução do operador no destino pode prosseguir somente quando o destino for conhecido no CA Process Automation. Selecione Desativado para permitir a pesquisa mais ampla. Selecione Ativado aqui e Desativado no próximo campo para a pesquisa mais restrita.

Observação: a pesquisa de DNS de um nome de host especificado localiza endereços IP associados; a pesquisa de DNS do endereço IP localiza nomes de host associados.

Valores: esta propriedade possui os seguintes valores:

- **Herdar do ambiente** - Usar o valor configurado para este campo nas propriedades do ambiente.
- **Ativado** - O escopo da pesquisa depende se o campo Pesquisar DNS ao fazer correspondência com o destino em grupos de hosts está ativado ou desativado.

  Se uma pesquisa de DNS estiver desativada, pesquisa: referência de grupo de hosts para um host remoto (exatamente)

  Se uma pesquisa de DNS estiver ativada, pesquisa: referência de grupo de hosts para um host remoto (exatamente ou resultado de pesquisa de DNS)
- **Desativado** - Pesquisar os componentes do domínio na seguinte ordem:

  Touchpoint (exatamente ou resultado de pesquisa de DNS)

  Orquestrador (exatamente ou resultado de pesquisa de DNS)

  Agente (exatamente ou resultado de pesquisa de DNS)

  Mapeamento de touchpoint do proxy para um host remoto (exatamente ou resultado de pesquisa de DNS)

  Referência de grupo de hosts para um host remoto (exatamente ou resultado de pesquisa de DNS)

Padrão: Herdar do ambiente.

Pesquisar DNS ao fazer correspondência com o destino em grupos de hosts?

Observação: esse campo é ativado quando Fazer correspondência do destino apenas em grupos de hosts estiver definido como Ativado.

Especifica se é necessário limitar a pesquisa pelas referências de grupo de hosts para o tipo de entrada. Por exemplo: quando o tipo de entrada do campo Destino for um FQDN, pesquisa apenas padrões de nomes de hosts. Quando o tipo de entrada do campo Destino for um endereço IP, pesquisa apenas sub-redes. Quando uma pesquisa de DNS for incluída, a pesquisa também poderá aceitar uma referência de grupo de hosts para o outro tipo, como resolvido por uma pesquisa de DNS.

Valores: esta propriedade possui os seguintes valores:

- **Herdar do ambiente** - Usar o valor configurado para este campo nas propriedades do ambiente.
- **Ativado** - Pesquisar todas as referências de grupo de hosts. As referências de grupo de hosts para nomes de host são padrões (expressões regulares) que podem incluir o nome de host especificado. As referências de grupo de hosts para endereços IP são sub-redes do endereço IP que são expressas em notação CIDR que pode incluir o endereço IP especificado. Estender a pesquisa a todas as referências de grupo de hosts. Permite que a pesquisa encontre uma correspondência exata ou uma correspondência para o resultado de pesquisa de DNS.
- **Desativado** - Restringir a pesquisa às referências de grupo de hosts que incluem uma correspondência exata para a entrada do campo Destino.

Padrão: Herdar do ambiente.

6. Clique em Salvar.
7. Clique em Desbloquear.

Substituir configurações de categoria de operador herdadas do ambiente

As configurações de categoria de operador são definidas na guia Módulos. As configurações de categoria de operador que foram definidas no nível do ambiente ou herdadas de configurações definidas no nível do domínio são exibidas como Herdar do ambiente. Um administrador com direitos de Administrador de configuração do ambiente pode ativar qualquer categoria de operador e substituir as configurações herdadas no nível do orquestrador.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a paleta Orquestradores.
3. Selecione o orquestrador que deseja configurar e clique em Bloquear.
4. Clique na guia Módulos.
5. Selecione uma categoria de operador, clique em Herdar do ambiente e selecione Ativar na lista suspensa.

   Observação: você pode desativar uma categoria de operador no nível do orquestrador selecionando Desativado na lista suspensa.
6. Clique com o botão direito do mouse na categoria do operador e selecione Editar.

   As configurações são exibidas.
7. Altere uma ou mais configurações herdadas.

   Observação: consulte Configurando categorias do operador (na página 270) para obter detalhes.
8. Clique em Salvar e fechar.

   Os valores configurados na caixa de diálogo aberta são salvos.
9. Clique no botão Salvar da barra de ferramentas.

   As alterações salvas são aplicadas à configuração do CA Process Automation.
10. Repita as etapas de 5 a 9 para cada categoria de operador a ser atualizada.
11. Selecione o orquestrador configurado e clique em Desbloquear.

Ativar disparadores para um Orquestrador

Um administrador com direitos de configuração do ambiente pode gerenciar disparadores no nível do orquestrador. Ative um disparador selecionado alterando seu status para Herdar do ambiente ou alterando seu status para Ativado e substituindo as configurações exibidas. Para exibir as configurações atuais de um disparador, você deve alterar o status para Ativado e selecionar Editar. Se você aceitar as configurações, configure os disparadores para Herdar do ambiente. Se você não aceitar as configurações porque elas estão incompletas ou não forem apropriadas para esse orquestrador, será possível configurar os campos e manter o status como Ativado.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a paleta Orquestradores.
3. Clique com o botão direito do mouse no Orquestrador selecionado e selecione bloquear.
4. Clique na guia Disparadores.

   Se os disparadores não forem configurados no Orquestrador, eles estarão com seu status desativado.
5. Clique com o botão direito do mouse no disparador que deseja examinar e clique em Editar.

   Os campos são exibidos com os valores que você pode usar como estão ou alterar.
6. Se o disparador estiver totalmente configurado com os valores que você deseja que o orquestrador selecionado use, selecione a opção Herdar do ambiente na lista suspensa e clique em Fechar.
7. Se o disparador não estiver totalmente configurado ou você desejar especificar valores de diferença para o orquestrador selecionado, faça o seguinte:

   a. Selecione Ativado na lista suspensa Ativar/desativar.

   b. Para obter descrições dos campos e outras informações pertinentes sobre cada um dos disparadores, consulte Administrar disparadores (na página 313).

   c. Se o disparador selecionado for o disparador de email e o Orquestrador não for o Orquestrador de domínio, clique em Procurar e selecione o arquivo de processo padrão.

      O campo Processo padrão do disparador é preenchido com o caminho correto para esse Orquestrador.

   d. Clique em Fechar
8. Clique em Salvar.
9. Clique com o botão direito do mouse no orquestrador bloqueado e clique em Desbloquear.

Configurar as diretivas do Orquestrador

As configurações das diretivas do orquestrador especificam as configurações de histórico para os processos executados no orquestrador. Elas também especificam a programação padrão e o processo padrão na biblioteca. Você pode configurar diretivas separadas para separar os orquestradores.

Siga estas etapas:

1. Clique na guia Configuração.
2. Em Navegador de configuração, selecione o orquestrador a ser configurado e clique em Bloquear.
3. Clique na guia Diretivas.
4. Selecione se deseja permitir que os usuários salvem um objeto editado como a mesma versão ao disponibilizar ou automatizem o controle de versão de objeto com a criação de uma nova versão ao disponibilizar.
5. Se você tiver definido um processo que especifica os manipuladores de processo padrão com regras de alteração de rotas e manipulação de exceções, vá até esse processo e selecione-o.
6. Especifique os requisitos para reter as instâncias de processos que foram executadas.
   a. Selecione o número mínimo de dias para salvar as instâncias de processo que foram executadas em um touchpoint ou em um host remoto. Se você configurar um dia, o processo continuará na biblioteca por no mínimo 24 horas antes de ser arquivado.
   b. Selecione o número mínimo de instâncias com falha de um processo a serem mantidas no histórico.
   c. Selecione o número mínimo de instâncias concluídas do objeto de processo a serem mantidas no histórico.
   d. Selecione o número máximo de mensagens de log que podem ser exibidas quando a instância do processo é aberta em uma exibição de processos.
7. Selecione o número mínimo de dias para armazenar um anexo no banco de dados do CA Process Automation antes de excluí-lo.

   Os usuários podem usar serviços web para disparar processos. Um usuário pode iniciar diretamente um processo ou agendar um formulário de solicitação inicial. Os usuários podem enviar arquivos como anexos nas chamadas de serviços web. Quando uma chamada de serviço web dispara um processo, os usuários podem acessar os arquivos desse processo. Um usuário pode usar o operador SOAP para encaminhar um anexo para a chamada de serviços web de saída.

8. Especifique os requisitos para eliminar as instâncias de processo que foram executadas no orquestrador selecionado e posteriormente arquivadas. Como alternativa, é possível eliminar as instâncias de processo que foram iniciadas em um determinado intervalo de dados, sob demanda.

   a. Defina a diretiva para limpar dados arquivados. As opções incluem:

      Não limpar dados arquivados

      As instâncias de processo arquivadas são mantidas até serem limpas manualmente.

      Eliminar dados arquivados diariamente

      Limpar instâncias de processo arquivadas como uma tarefa programada, de acordo com as configurações dos dois campos a seguir.

      Eliminar dados sem arquivar

      As instâncias do processo são mantidas como ativas durante um intervalo configurado. Quando esse intervalo passar, os dados serão limpos. Nenhuma instância do processo é arquivada.

   b. Defina a hora (no formato hh:mm) em que são limpas as instâncias arquivadas que foram mantidas durante o número de dias configurado.

   c. Defina o número de dias para manter instâncias do processo arquivadas. Após uma instância arquivada ser mantida durante o número de dias configurado, ela é limpa na hora especificada.

   d. Para limpar as instâncias arquivadas que foram iniciadas em um intervalo de tempo especificado no orquestrador atual, clique no botão Excluir instância arquivada, selecione um intervalo de datas e clique em OK.

9. Especifique se deve ser exigida autenticação quando um usuário tentar acessar anexos fora do CA Process Automation. Se essa opção estiver selecionada, o usuário deverá fornecer credenciais válidas para acessar os anexos.

10. Especifique se é necessário aplicar a segurança em tempo de execução. Se selecionado, a segurança em tempo de execução é ativada para os processos definidos como Ativar ou que herdam uma configuração ativada.

    Observação: se você selecionar a opção Ativar a segurança em tempo de execução e selecionar Executar como proprietário como a opção Segurança em tempo de execução para um processo, use a opção Definir proprietário para estabelecer a propriedade de cada objeto de processo afetado. Para obter mais informações, consulte a ajuda online ou o *Guia do Criador de Conteúdo*.

11. Clique em Salvar.

12. Clique em Desbloquear.

Configurar espelhamento do Orquestrador

Os orquestradores espelham dados e informações de configuração armazenados no orquestrador de domínio. A configuração de espelhamento especifica a frequência em que um orquestrador verifica alterações no orquestrador de domínio. As alterações no orquestrador de domínio são aplicadas ao orquestrador no host local. Você pode definir o intervalo de espelhamento em um orquestrador.

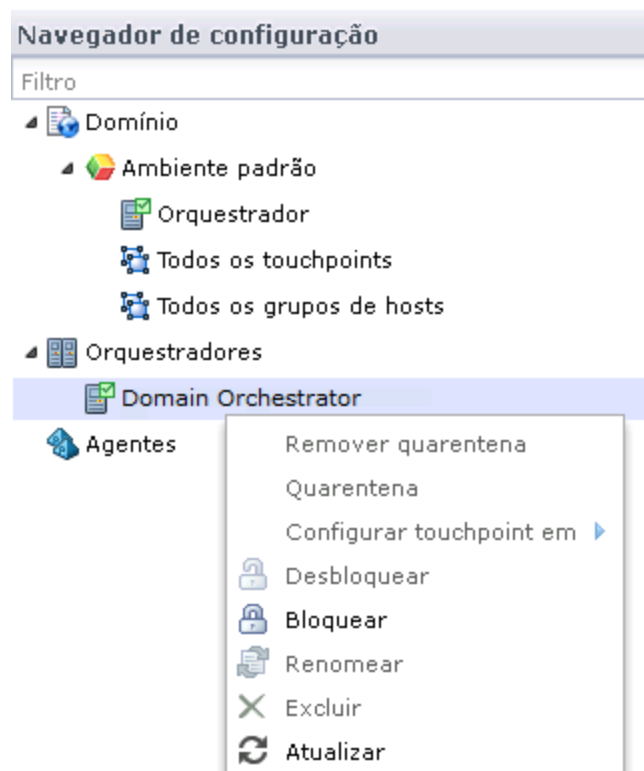
Quando você seleciona um orquestrador agrupado, o intervalo definido se aplica ao espelhamento de todos os nós ativos no agrupamento. Um nó de agrupamento pode estar inativo quando outros nós no agrupamento forem atualizados. Nesse caso, o espelhamento ocorrerá para o nó inativo quando ele for iniciado.

Observação: é possível carregar um arquivo JAR para a pasta Recursos do orquestrador no orquestrador de domínio. Quando você reiniciar o orquestrador de domínio, o CA Process Automation implantará o arquivo no orquestrador de domínio. O orquestrador de domínio espelha (copia) o arquivo no intervalo de espelhamento configurado, após o qual reiniciam-se os outros orquestradores. Quando os orquestradores reiniciam, o arquivo espelhado fica disponível para uso.

Siga estas etapas:

1. Clique na guia Configuração.
2. Na paleta Navegador de configuração, expanda Orquestradores.
3. Selecione o orquestrador a ser configurado e clique em Bloquear.
4. Clique na guia Espelhamento.
5. No campo Intervalo de espelhamento (minutos), selecione o intervalo entre os momentos em que o orquestrador selecionado solicita atualizações do orquestrador de domínio. O produto espelha todas as alterações no orquestrador selecionado no intervalo especificado.
6. Clique em Salvar.
7. Na paleta Navegador de configuração, selecione o orquestrador configurado e clique em Desbloquear.

Manter o host do orquestrador

Quando você seleciona um orquestrador no nó Orquestradores, os detalhes exibidos são relevantes para o host, e não para seu touchpoint.

Consulte os tópicos a seguir, associados às opções de menu do host do orquestrador.

- Remover quarentena

  Consulte Remover a quarentena de um orquestrador (na página 192).

- Quarentena

  Consulte Colocar um orquestrador em quarentena (na página 191).

- Configurar touchpoint em

  Consulte Configurar as propriedades do touchpoint de orquestrador (na página 174).

- Desbloquear - selecione o orquestrador e clique em Desbloquear.
- Bloquear - selecione o orquestrador e clique em Bloquear.
- Renomear - selecione o orquestrador e digite um novo nome.
- Excluir - selecione o orquestrador e clique em Excluir. Não é possível excluir o orquestrador de domínio.
- Atualizar - selecione o orquestrador e clique em Atualizar.

Colocar um Orquestrador em quarentena

Você pode colocar em quarentena qualquer Orquestrador, exceto o Orquestrador de domínio. Colocar em quarentena isola o orquestrador. Os operadores não podem ser executados em um orquestrador que foi colocado em quarentena. Não é possível abrir a biblioteca de um orquestrador em quarentena. Por isso, não é possível criar ou salvar objetos da biblioteca em um orquestrador em quarentena.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito e selecione Bloquear.
3. Clique com o botão direito do mouse no ambiente que contém o orquestrador que você deseja colocar em quarentena e selecione Bloquear.
4. Expanda o nó Orquestradores.
5. Clique com o botão direito no Orquestrador que você deseja colocar em quarentena e selecione Bloquear.
6. Clique com o botão direito do mouse no orquestrador novamente e selecione Quarentena.

7. Clique em Salvar.
8. Clique com o botão direito do mouse no orquestrador e selecione Desbloquear.
9. Clique com o botão direito do mouse no ambiente bloqueado e selecione Desbloquear.
10. Clique com o botão direito do mouse no domínio e selecione Desbloquear.

Remover a quarentena de um orquestrador

Se a quarentena tiver sido criada por um motivo que não seja a remoção do orquestrador, remova a quarentena do orquestrador quando não houver mais necessidade de quarentena.

Para remover a quarentena de um Orquestrador

1. Clique na guia Configuração.
2. Expanda a paleta Orquestradores.
3. Clique com o botão direito do mouse no orquestrador de destino em quarentena e clique em Bloquear.
4. Clique com o botão direito no Orquestrador novamente e clique em Remover quarentena.
5. Clique com o botão direito do mouse no orquestrador e selecione Desbloquear.

   A caixa de diálogo Dados não salvos é exibida, perguntando se você deseja salvar as alterações.
6. Clique em Sim.

Interromper o orquestrador

Apenas administradores com credenciais de administrador no servidor onde o orquestrador está instalado podem interromper o orquestrador.

Importante: se um orquestrador não for desligado corretamente, a seguinte pasta temporária poderá acumular vários gigabytes de arquivos. Se isso acontecer, você pode excluir a pasta tmp com segurança:

`install_dir/server/c2o/tmp`

Siga estas etapas:

1. Usando credenciais de Administrador, efetue logon no host em que o Orquestrador de destino está instalado.
2. Se estiver conectado a um host do Windows, você pode interromper o serviço do orquestrador no menu Iniciar, na janela Serviços, ou na linha de comando. Realize uma da seguintes ações:
   - No menu Iniciar, selecione Programas, CA, CA Process Automation 4.0 e Interromper serviço do orquestrador.
   - Selecione Ferramentas Administrativas e Serviços no Painel de Controle. Selecione o seguinte serviço e clique em Interromper:

     ```
     Orquestrador do CA Process Automation (C:\Arquivos de
     Programas/CA/PAM/server/c2o)
     ```
   - Abra um prompt de comando e execute o seguinte script:

     ```
     install_dir/server/c2o/bin/stopc2osvc.bat
     ```
3. Se você estiver conectado a um host do UNIX ou Linux, execute as seguintes etapas:
   a. Altere os diretórios para ${PAM_HOME}/server/c2o/. Por exemplo, altere os diretórios para:

      ```
      /usr/local/CA/PAM/server/c2o
      ```
   b. Execute o script c2osvrd.sh com a opção stop. Por exemplo:

      ```
      ./c2osvrd.sh stop
      ```

Iniciar o orquestrador

Apenas administradores com credenciais de administrador no servidor onde o orquestrador está instalado podem reiniciar o serviço do orquestrador.

Siga estas etapas:

1. Usando as credenciais de administrador, efetue logon no host em que o orquestrador de destino está instalado.
2. Se estiver conectado a um host do Windows, você pode reiniciar o serviço do orquestrador no menu Iniciar, na janela Serviços, ou na linha de comando. Execute uma das tarefas a seguir:
   - Selecione Programas, CA, CA Process Automation e Iniciar serviço do orquestrador, no menu Iniciar.
   - Selecione Ferramentas Administrativas e Serviços no Painel de Controle. Selecione o seguinte serviço e clique em Iniciar:

     ```
     Orquestrador do CA Process Automation (C:\Arquivos de
     Programas/CA/PAM/server/c2o)
     ```
   - Abra um prompt de comando e execute o seguinte script:

     install_dir/server/c2o/bin/startc2osvc.bat
3. Se você estiver conectado a um host do UNIX ou Linux, execute as seguintes tarefas:

   a. Altere os diretórios para ${PAM_HOME}/server/c2o/. Por exemplo, altere os diretórios para:

      ```
      /usr/local/CA/PAM/server/c2o
      ```

   b. Execute o script c2osvrd.sh com a opção start. Ou seja, execute:

      ```
      ./c2osvrd.sh start
      ```

Observação: após iniciar o serviço para o orquestrador de domínio, inicie o CA Process Automation.

Eliminar instâncias de processo arquivadas de um orquestrador

É possível limpar sob demanda as instâncias de processo executadas durante um intervalo de datas especificado.

Limpe as instâncias de processo arquivadas do banco de dados de tempo de execução de um orquestrador nas seguintes situações:

- Você precisa de mais espaço disponível; o acúmulo de instâncias arquivadas está causando degradação do desempenho.
- Você definiu a diretiva do orquestrador para desativar a limpeza automática.

Siga estas etapas:

1. Clique na guia Configuração e expanda o nó Orquestradores no Navegador de configuração.

   O nó expandido mostra todos os orquestradores no domínio.

2. Clique com o botão direito do mouse no orquestrador com as instâncias de processo arquivadas que você deseja limpar e clique em Bloquear.

3. Clique na guia Diretivas.

4. Clique no botão Excluir instância arquivada, na parte inferior do painel.

5. Na caixa de diálogo Excluir instância arquivada, defina o intervalo de datas cujas instâncias devem ser limpas.

   a. Clique no botão de calendário A partir da data e selecione Hoje ou uma data de início anterior à de hoje.

   b. Clique no botão de calendário Até a data e selecione Hoje ou uma data de término posterior à de hoje.

   c. Clique em OK.

6. Clique em Sim na mensagem de confirmação.

   O processo de limpeza excluirá todas as instâncias arquivadas executadas durante o intervalo de datas especificado.

7. Clique com o botão direito do mouse no orquestrador e clique em Desbloquear.

Capítulo 8: Administrar agentes

Um agente é um componente que deve ser instalado em vários hosts em cada ambiente. Após instalar um agente em um host, configure um touchpoint (uma entidade lógica) que associa o ambiente atual ao host do agente.

Os agentes oferecem suporte à execução de processos. Os processos são compostos de operadores. A maioria dos operadores é executada no Orquestrador. Quando um operador é executado em um host do agente, ele faz isso na direção do Orquestrador e retorna os resultados para o Orquestrador. O Orquestrador executa o processo principal.

Para garantir que um host do agente esteja sempre disponível para o processamento, associe vários hosts do agente a um único touchpoint. Um touchpoint associa um ou mais agentes a um ambiente especificado. Os criadores de conteúdo geralmente definem como destino um host do agente escolhendo o seu touchpoint como destino.

Para executar operadores em hosts remotos que não tenham nenhum agente, associe um agente a touchpoints do proxy ou grupos de hosts. Os operadores podem ser executados em um host remoto que não tenha nenhum agente quando uma conexão SSH está configurada do host do agente para o host remoto de destino. Para serem executados em um host remoto, os operadores definem como destino o touchpoint do proxy.

Para obter informações sobre como configurar a tolerância a falhas (configurações de prioridade) ou o balanceamento de carga entre os agentes associados ao mesmo touchpoint, consulte Administrar touchpoints (na página 219).

Para obter informações sobre o estabelecimento de conexões SSH, consulte Administrar touchpoints do proxy (na página 239) e Administrar grupos de hosts (na página 247).

Esta seção contém os seguintes tópicos:

Configurar os agentes para suportar os destinos do operador

A configuração do agente em um ambiente de criação é geralmente limitado à definição de um pequeno conjunto de touchpoints, cada um mapeado para um único agente. Se os hosts apresentarem fornecimento baixo, você poderá associar vários touchpoints ao mesmo agente.

Configurações de agente mais robustas são típicas de ambientes de produção. Seis opções são apresentadas primeiro separadamente e, em seguida, em uma tabela de resumo para referência. Use esses detalhes para planejar e implementar a configuração do agente no ambiente de produção.

O operador é executado em um host de agente específico.

Essa opção é a mais fácil de implementar durante a execução de um operador em um host com um agente. Essa opção é aceitável em um ambiente de teste ou de desenvolvimento.

Destino real

Nome do host ou endereço IP do destino.

Requisitos de instalação

Instale um agente no host de destino.

Requisitos de associação

Defina um touchpoint que associe um agente com o ambiente de produção.

Destino do operador

Digite o nome do touchpoint. Se preferir, você pode inserir a ID do agente.

O operador é executado em um dos possíveis agentes de prioridade mais alta.

Essa opção permite especificar que o operador seja executado no host mais desejável se ele estiver disponível. Em caso negativo, no próximo host mais desejável. Você decide o que torna um host mais desejável do que o outro. Você pode configurar um touchpoint para que um determinado operador seja sempre executado no host com a maior capacidade. Ou, então, você pode reservar esses hosts e usá-los para execução apenas se todos os outros candidatos estiverem ocupados.

Destino real

Desconhecido. Registre os nomes de host dos hosts de destino candidatos, por ordem de preferência.

Requisitos de instalação

Instalar um agente em cada host de destino candidato.

Requisitos de associação

Defina um touchpoint e associá-lo a todos os hosts de destino candidatos. Na definição do touchpoint, especifique a classificação de prioridade para cada um.

Destino do operador

Digite o nome do touchpoint.

O operador é executado em um dos vários possíveis agentes menos ocupado.

Essa opção demora mais tempo para implementar do que um touchpoint associado com um agente, mas é uma opção avançada quando o destino for um host com um agente. Essa opção foi criada para um ambiente de produção, onde é importante que o processo seja executado na hora programada.

Destino real

Desconhecido. Registrar os nomes de host dos hosts de destino candidatos.

Requisitos de instalação

Instalar um agente em cada host de destino candidato.

Requisitos de associação

Defina um touchpoint e associá-lo a todos os hosts de destino candidatos. Na definição do touchpoint, digite o mesmo número da prioridade para cada associação. Essa implementação é para balanceamento de carga.

Destino do operador

Digite o nome do touchpoint.

O operador é executado em vários hosts de agente ao mesmo tempo.

O uso do grupo de touchpoints permite que você execute um operador simultaneamente em todos os hosts associados aos touchpoints do grupo.

Destinos reais

Registre o nome do host de cada host de destino.

Requisitos de instalação

Instalar um agente em cada host de destino.

Requisitos de associação

- Definir um touchpoint separado para cada um desses agentes.
- Defina um grupo de touchpoints composto desses touchpoints.

Destino do operador

Digite o nome do grupo de touchpoints.

O operador é executado em um host remoto específico.

Às vezes, não é possível instalar um agente em um host a ser definido como destino de um operador. Nesse caso, defina um agente como o touchpoint do proxy. Crie uma conexão SSH do host com o agente até o host remoto de destino.

Destino real

Registre o nome do host ou endereço IP do host remoto de destino.

Ativando o host de origem

Registre o nome de host do host de origem que pode se conectar ao destino com uma conexão SSH.

Requisitos de conectividade

Criar a conexão SSH do host de origem para o host remoto.

Requisitos de instalação

Instale um agente no host de origem.

Requisitos de associação

Defina um touchpoint do proxy no host de origem e especificar os detalhes da conexão para o host remoto de destino.

Destino do operador

Digite o nome do touchpoint do proxy.

O operador é executado em um host remoto, em que o destino pode ser alterado em cada execução.

Essa opção permite que você decida qual host remoto será usado como destino imediatamente antes do tempo de execução, quando você especificar o destino com seu nome de host ou endereço IP. O destino deve ser um integrante de um grupo de hosts. Um grupo de hosts é um grupo com um padrão de nome de host comum ou um padrão de endereço IP comum. Os hosts com um padrão de endereço IP comum pertencem à mesma sub-rede.

Destino real

Desconhecido. Registre os nomes de host dos hosts remotos de destino candidatos.

Ativando o host de origem

Registre o nome de host do host de origem que pode se conectar a cada um dos destinos candidatos com uma conexão SSH.

Requisitos de conectividade

Crie a conexão SSH do host de origem para cada host remoto.

Requisitos de instalação

Instale um agente no host de origem.

Requisitos de associação

Defina um grupo de hosts no host de origem com um padrão que os hosts remotos tenham em comum.

Destino do operador

Digite o nome do host ou endereço IP do host remoto de destino. Expresse o destino do operador em um conjunto de dados. É possível modificar os conjuntos de dados, mesmo quando forem importados com um processo que não pode ser modificado.

Use a tabela a seguir como guia para criar tabelas de resumo para você. Documentação em forma de tabelas de resumo podem ajudar outros usuários a encontrar essas informações quando você não estiver disponível.

Tipo de destino	Associação do agente	Outra configuração	Destino do operador
Um único host	Um novo touchpoint	N/D	Nome do touchpoint
Um de vários hosts, em ordem de prioridade	Um touchpoint existente	Especifique a prioridade para selecionar o host de destino.	Nome do touchpoint
Um dos vários hosts (sem prioridade)	Um touchpoint existente	Atribua a mesma prioridade a cada host de destino candidato.	Nome do touchpoint

Tipo de destino	Associação do agente	Outra configuração	Destino do operador
Vários hosts ao mesmo tempo	Um novo touchpoint	Crie um grupo de touchpoints com todos os touchpoints.	Nome do grupo de touchpoints
Um único host remoto	Um touchpoint do proxy	Crie uma conexão SSH do host do agente com o host de destino remoto.	Nome do touchpoint do proxy
Um de vários hosts remotos	Um grupo de hosts	Crie uma conexão SSH do host do agente com cada host de destino remoto.	Nome de host de destino ou endereço IP

Mais informações

Sobre a comunicação do agente (na página 217)

Instalar um agente de forma interativa

Os processos podem incluir operadores que precisam ser executados em servidores com um aplicativo, banco de dados ou sistema de destino. Se possível, instale um agente nesse tipo de servidor. Se não for possível, instale o agente em um host que possa se conectar a esse servidor por meio de SSH.

Importante: Antes de instalar um agente, verifique se o Orquestrador de domínio está em execução.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique na paleta Instalação.
3. Clique em Instalar para instalar o agente.

   Uma caixa de diálogo é exibida, mostrando o andamento do download do aplicativo.
4. Se você receber um aviso de segurança, clicar em Executar.

   A caixa de diálogo Seleção de idioma é aberta. O idioma do computador host é selecionado por padrão.
5. Clique em OK ou selecione outro idioma e clique em OK.

   A página de boas-vindas do assistente de instalação do agente do CA Process Automation é exibida.
6. Clique em Avançar.

   O Contrato de Licença é exibido.

7. Leia a licença. Se você aceitar os termos, clique em Eu aceito os termos do Contrato de Licença. Clique em Avançar.

   A página Defina o Java Home Directory é aberta.

8. Se o diretório inicial do Java não for exibido corretamente, procure a pasta JRE.

   Todas as plataformas oferecem suporte à versão jre6; o Windows oferece suporte às versões jre6 e jre7.

   Veja o seguinte exemplo de caminho para a plataforma Windows:

   ```
   C:\Arquivos de programas\Java\jdk1.7.0_45
   ```

9. Clique em Avançar.

   A página Selecionar o diretório de destino é exibida. Em hosts do Windows, o caminho padrão é:

   ```
   C:\Program Files\CA\PAM Agent
   ```

10. Clique em Avançar para aceitar o padrão ou digite um diretório de destino para o novo agente e clique em Avançar.

    A página Selecionar pasta do menu Iniciar é exibida.

11. (Somente no Windows) Clique em Avançar para aceitar o agente do CA Process Automation como o atalho do menu Iniciar ou digite um novo nome e clique em Avançar.

    ■ (Opcional) Crie atalhos para todos os usuários nesse host.

    ■ (Opcional) Não criar uma pasta no menu Iniciar.

12. Examine o URL do domínio. Este é o URL a partir do qual você iniciou a instalação do agente. Clique em Avançar.

13. Se o domínio estiver protegido, forneça uma senha.
14. Preencha a página Propriedades gerais e, em seguida, clique em Avançar.
    a. Digite o nome do host do agente para Host do agente. Esse nome identifica o host a partir do qual você iniciou a instalação.
    b. Altere ou aceite o Nome de exibição padrão, o nome do host.
    c. Se você tiver iniciado a instalação do agente em um host do Windows, selecione Instalar como um serviço do Windows.
    d. Para forçar uma nova conexão para cada comunicação de um orquestrador a um agente, selecione Usar comunicação obsoleta.

       Recomendamos deixar essa caixa de seleção *desmarcada*. A comunicação simplificada, o padrão, é preferencial porque usa uma conexão persistente.
    e. Se você tiver selecionado Usar comunicação obsoleta, aceite 7003 como a Porta do agente, a menos que essa porta esteja em uso. Se a porta padrão estiver em uso, digite um número de porta sem uso, como 57003, como a porta na qual o agente escuta a comunicação com os orquestradores.

       Observação: se a comunicação obsoleta não for usada, os orquestradores usarão uma conexão de soquete da web (estabelecida por agentes) para se comunicar com os agentes. Os orquestradores usam a porta 80 para se comunicar com agentes por HTTP. Os orquestradores usam a porta 443 para se comunicar com agentes por HTTPS.
    f. Selecione Iniciar agente após a instalação.

       A inicialização do agente permite exibir o agente ativo e continuar com a configuração do agente.
15. Clique em Avançar para aceitar o diretório temporário padrão para executar os scripts ou digite outro caminho e, em seguida, clique em Avançar.

    Observação: um caminho aceitável não contém espaços.

    A página Definir a diretiva de execução do PowerShell é exibida.
16. Preencha a configuração de uma das seguintes maneiras.
    - Para executar os scripts do Windows PowerShell por meio desse agente:
        a. Marque a caixa de seleção Definir a diretiva de execução do PowerShell.
        b. Vá até o local do host do PowerShell, se for diferente do padrão exibido.
        c. Clique em Avançar.
    - Se você não usar o Windows PowerShell, clique em Avançar.

    A instalação do agente é iniciada.
17. Clique em Concluir.
18. (Somente no Windows) Inicie o serviço do agente. Clique em Iniciar, Programas, CA, Agente do CA Process Automation, Iniciar serviço do agente.

19. Clique na paleta Navegador de configuração, na guia Configuração.
20. Clique em Atualizar. (Ou, efetue logoff e logon novamente.)
21. Expanda Agentes e verifique se o nome do seu agente está listado.

    Observação: para usar o host do agente como um destino, configure um touchpoint. Para usar o agente do host como um gateway para um host remoto, configure um touchpoint do proxy.

Adicionar um touchpoint de agente

Ao instalar um agente em um host, o nome de exibição do agente é exibido sob o nó Agentes. Para que um operador possa usar esse host como destino, você deve configurar um touchpoint que faça referência ao host.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o nó Agentes.
3. Clique com o botão direito do mouse no agente e selecione Configurar touchpoint em. Em seguida, escolha o *ambiente*.

   Um prompt para bloquear o ambiente selecionado é exibido.
4. Clique em Sim para bloquear o ambiente selecionado.

   A caixa de diálogo Adicionar touchpoint do agente é exibida.
5. Digite um nome para o novo touchpoint que seja diferente do nome do host e clique em OK.

   O novo touchpoint é exibido sob o nó Todos os touchpoints para o ambiente associado.
6. Clique em Salvar.
7. Selecione o ambiente bloqueado e clique em Desbloquear.

Adicionar um grupo de hosts do agente

Se um operador precisar usar como destino hosts remotos diretamente (com um endereço IP ou nome do host), você pode:

1. Criar um grupo de hosts. (na página 250)
2. Configurar as propriedades do grupo de hosts (na página 251). Você pode adicionar hosts remotos específicos ou digitar padrões que incluem os hosts de destino.
3. Crie credenciais de SSH em hosts em um grupo de hosts (na página 256). Ou seja, crie uma conta de usuário em cada host remoto com as credenciais digitadas nas propriedades do grupo de hosts.

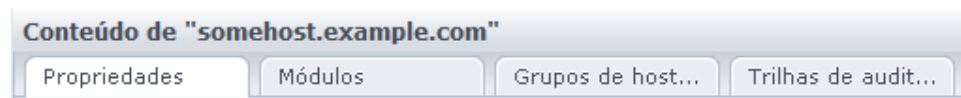
Mais informações:

Administrar grupos de hosts (na página 247)

Configurar o conteúdo de um agente selecionado

Muitas configurações de propriedades são recuperadas durante a instalação do agente. Os touchpoints associados são detalhes de configuração exclusivos aos agentes e não são herdados. As definições das configurações do operador na guia Módulos são herdadas por padrão. As configurações que você define para um agente são diferentes das configurações que você define para o touchpoint do agente.

Conteúdo de "somehost.example.com"

Propriedades | Módulos | Grupos de host... | Trilhas de audit...

O menu Agente tem as seguintes guias:

Propriedades

Consulte Configurar propriedades do agente (na página 207).

Módulos

Consulte Personalizar configurações do agente para categorias do operador (na página 208).

Touchpoints e grupos de hosts associados

Consulte Exibir os touchpoints e grupos de hosts de um agente selecionado (na página 210).

Trilhas de auditoria

Consulte Exibir a trilha de auditoria de um agente (na página 339).

Configurar propriedades do agente

É possível definir valores para as seguintes propriedades do agente:

- A frequência com que o agente envia um sinal de monitoramento para o orquestrador de domínio.
- A frequência com que o agente verifica o orquestrador de domínio em busca de atualizações.

O agente envia um sinal de monitoramento durante a inicialização e na programação configurada, enquanto o agente estiver ativo. O orquestrador de domínio confirma os sinais de monitoramento ou as atualizações do domínio, se disponíveis. O orquestrador de domínio envia atualizações espelhadas para o agente nos intervalos de espelhamento especificados.

Você pode definir as propriedades do agente no Navegador de configuração.

Siga estas etapas:

1. Clique na guia Configuração e expanda Agentes, na paleta Navegador de configuração.
2. Selecione o agente a ser configurado e clique em Bloquear.
3. Selecione a guia Propriedades para o agente selecionado.
4. (Opcional) Revise as seguintes propriedades somente leitura:
   - Status - Ativo ou Inativo
   - Nome do agente - nome configurado como Nome de exibição durante a instalação.
   - Nome do host - nome configurado como Host do agente durante a instalação.
   - Endereço do host
5. (Opcional) Atualize as seguintes propriedades:
   - Intervalo de espelhamento (minutos)
   - Intervalo entre sinais de monitoramento (minutos) - o valor padrão no nível de domínio é 2.
   - Usar comunicação obsoleta
6. Selecione o agente e clique em Desbloquear.
7. Clique em Sim na caixa de diálogo Dados não salvos para salvar as alterações.

Personalizar a categoria do operador para um agente selecionado

Todos os ambientes, Orquestradores e agentes herdam configurações definidas na guia Módulos do domínio. Os administradores podem editar a configuração nos níveis mais baixos da hierarquia de domínio. Os administradores podem também ativar as categorias de operadores em qualquer agente e podem editar as configurações conforme necessário.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda os agentes, clique com o botão direito do mouse no agente a ser personalizado e, em seguida, selecione Bloquear.
3. Clique na guia Módulos.
4. Selecione Ativado na lista suspensa Ativar/desativar para a categoria de operador a ser editada.
5. Clique com o botão direito do mouse na mesma categoria e selecione Editar.
6. Altere as configurações de propriedade da categoria selecionada para o agente escolhido. Para obter mais informações, consulte as seguintes descrições de campo no nível de domínio:
   - Configurar o Catalyst (na página 271).
   - Configurar Execução de comando (na página 277).
   - Configurar Bancos de dados: Propriedades do Oracle (na página 283).
   - Configurar Bancos de dados: Propriedades do servidor MSSQL (na página 285).
   - Configurar Bancos de dados: Propriedades do MySQL (na página 287).
   - Configurar Bancos de dados: Propriedades do Sybase (na página 288).
   - Configurar Serviços de diretório (na página 290).
   - Configurar Email (na página 292).
   - Configurar Gerenciamento de arquivos (na página 294).
   - Configurar Transferência de arquivos (na página 296).
   - Configurar Utilitários de rede (na página 298).
   - Configurar Controle de processo (na página 299).
   - Configurar Utilitários (na página 300).
   - Configurar Serviços web (na página 302).
7. Clique em Salvar e clique em OK na mensagem de verificação.
8. Clique com o botão direito do mouse no agente bloqueado e selecione Desbloquear.

Desativar uma categoria de operador em um agente selecionado

Na guia Módulos de um agente selecionado, é possível desativar uma ou mais categorias de operadores para esse agente.

Siga estas etapas:

1. Clique na guia Configuração e expanda Agentes, na paleta Navegador de configuração.
2. Selecione o agente a ser configurado e clique em Bloquear.
3. Clique na guia Módulos.
4. Selecione uma categoria de operador para a qual a opção Ativar/desativar esteja definida para Ativar ou Herdar do ambiente.
5. Selecione Desativar na lista suspensa Ativar/desativar.
6. Clique em Salvar.
7. Clique em Desbloquear.

   O produto desativa a categoria do operador selecionada no agente selecionado.

Configurar um touchpoint ou grupo de hosts selecionado

Um touchpoint é uma associação entre um agente (ou orquestrador) e um ambiente. Um touchpoint do proxy é uma associação entre um agente, um host remoto e um ambiente. Um grupo de hosts é uma associação entre um agente, um grupo de hosts remotos e um ambiente.

Quando você adiciona um touchpoint ou touchpoint do proxy a um agente, esse touchpoint é exibido em Todos os touchpoints.

Quando você adiciona um grupo de hosts a um agente, o nome desse grupo de hosts é exibido em Todos os grupos de hosts.

Consulte os tópicos a seguir para obter detalhes da configuração:

- Administrar touchpoints (na página 219).
- Administrar touchpoints do proxy (na página 239).
- Administrar grupos de hosts (na página 247).

Exibir os touchpoints e grupos de hosts de um agente selecionado

É possível exibir os touchpoints e grupos de hosts de um agente selecionado na guia Touchpoint associado.

Siga estas etapas:

1. Clique na guia Configuração e expanda Agentes, na paleta Navegador de configuração.
2. Selecione o agente para o qual deseja exibir touchpoints e grupos de hosts.
3. Clique na guia Touchpoint associado.

   Os nomes dos touchpoints ou grupos de hosts e a hierarquia (onde domínio é o nó raiz) são exibidos.

Colocar um Agente em quarentena

A quarentena isola um agente do tráfego de rede de entrada e de saída do CA Process Automation. Os operadores não podem ser executados em um agente em quarentena. Coloque um agente em quarentena sempre que desejar impedi-lo de ser o destino de um operador do CA Process Automation.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o nó Agentes.
3. Selecione o agente que deseja colocar em quarentena e clique em Bloquear.
4. Clique com o botão direito do mouse no agente e selecione Quarentena. O modificador de quarentena é adicionado ao ícone base do agente bloqueado.
5. Clique em Desbloquear.

   A caixa de diálogo Dados não salvos é exibida, perguntando se você deseja salvar as alterações.
6. Clique em Sim.

   O modificador de quarentena é exibido para o grupo de hosts ou touchpoints associado ao agente em quarentena.

Remover um Agente da quarentena

Quando o período de quarentena terminar, remova a quarentena do agente.

Siga estas etapas:

1. Clique na guia Configuração e expanda o nó Agentes.
2. Clique no agente em quarentena para o qual deseja remover a quarentena e clique em Bloquear.
3. Clique com o botão direito do mouse no agente e clique em Remover quarentena.
4. Clique em Desbloquear.

   A caixa de diálogo Dados não salvos é exibida, perguntando se você deseja salvar as alterações.
5. Clique em Sim.

   O modificador de bloqueio do ícone base do agente é removido. Os modificadores de quarentena do agente e os ícones base do grupo de hosts ou touchpoints associado são substituídos pelo modificador de ícone ativo.

Renomear um Agente

O nome de um agente é padronizado para o nome do host durante o processo de instalação do agente. É possível renomear o agente. Por exemplo, você pode substituir o FQDN do host por Agente-*nome_do_host*.

Siga estas etapas:

1. Clique na guia Configuração e expanda Agentes, na paleta Navegador de configuração.
2. Selecione o agente a ser renomeado e clique em Bloquear.
3. Clique com o botão direito do mouse no agente e selecione Renomear.
4. Digite o novo nome.
5. Clique em Salvar.
6. Selecione o agente e clique em Desbloquear.

Identificar o caminho de instalação de um agente

É possível identificar o caminho onde o agente está instalado. O caminho padrão para o sistema operacional Windows 7 é:

```
C:\Arquivos de programas (x86)\CA\Pam Agent\PAMAgent
```

Execute esta etapa:

Use o script a seguir para identificar o caminho de instalação do agente:

```
echo %C2OHOME%
```

O script retorna o caminho completo de instalação do agente do CA Process Automation.

Observação: esse script pressupõe que C2OHOME foi definido como uma variável de ambiente.

Gerenciar o encerramento de um host com um Agente

Quando for notificado de que sua empresa planeja substituir o hardware em que você instalou agentes, considere o seguinte processo para minimizar o impacto. Esse processo reatribui os touchpoints originais aos agentes instalados em novos itens de hardware. A reatribuição permite que os processos que dependem desses touchpoints continuem sendo executados sem modificação.

Dois cenários comuns são:

- Os antigos hosts são removidos e, em seguida, os novos são adicionados. Essa prática é comum quando os endereços IP são reatribuídos.
- O novo host é adicionado e, em seguida, o antigo é removido.

Caso o plano seja remover hosts antigos antes de implantar novos, considere a seguinte abordagem:

1. Faça o seguinte antes que um host seja removido da rede:
   a. Identificar o nome do agente no CA Process Automation para o host que está sendo encerrado.

      A paleta Agentes no Navegador de configuração relaciona todos os Agentes com seus status.
   b. Identificar os touchpoints associados ao agente a ser excluído.

      Na paleta Agentes no navegador de configuração, selecione o agente e clique na guia Touchpoints associados para exibir a lista de touchpoints cuja reatribuição deve ser avaliada.
   c. Desinstale o software de agente do host que está sendo encerrado ou remodelado.
2. Instalar o software de Agente no host que substitui o host encerrado.
3. Associe o touchpoint afetado ao novo agente.
4. Remova o agente do host encerrado no CA Process Automation.

   Na paleta Agentes no Navegador de configuração, clique com o botão direito no agente, selecione Bloquear e, em seguida, clique com o botão direito e selecione Excluir.

Caso novos hosts sejam colocados na rede antes que os antigos sejam retirados, considere a seguinte abordagem:

1. Instalar um agente em cada novo host.
2. Associar os touchpoints afetados a novos agentes.
3. Usar Remoção em massa do agente para remover os agentes que foram substituídos.

Excluir um agente

Quando não desejar mais um agente instalado por você, desinstale-o do host. Em seguida, exclua-o da paleta Agentes.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Expanda a opção Agentes e verifique se o agente de destino está desbloqueado e não está em quarentena.
3. Selecione o agente de destino e clique em Excluir.

   Uma caixa de diálogo de confirmação aparece.

4. Clique em OK.
5. Clique em Salvar.
6. Selecione Domínio e clique em Desbloquear.

Remover Agentes selecionados em massa

Quando os servidores usados para os agentes forem encerrados, você pode remover as referências do CA Process Automation a esses agentes inativos em massa. Em seguida, você pode remover, em massa, os touchpoints associados vazios.

Quando a substituição de servidores é feita em uma sub-rede de cada vez, é possível selecionar os agentes associados para remoção especificando uma pesquisa baseada no CIDR. Se os servidores que estão sendo encerrados possuírem um padrão comum em seus nomes de host, você poderá selecionar agentes para a remoção com base em um determinado critério de correspondência de padrões.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito do mouse em Domínio e selecione Bloquear.
3. Clique com o botão direito do mouse em Domínio e selecione Remoção de agente em massa.
4. Digite os critérios de pesquisa de uma das seguintes maneiras:
   - Selecione Pesquisar padrão do endereço IP e digite uma sub-rede no formato CIDR que contenha os endereços IP de destino.
   - Selecione Pesquisa por padrão de nome de host e digite uma expressão de pesquisa que inclua o nome do domínio, por exemplo, *.*minhaempresa*.com.
   - Selecione um dos padrões, mas deixe o campo de pesquisa em branco.
5. Clique em Pesquisar.

   A tabela Agentes exibe todos os agentes que correspondem aos critérios de pesquisa, mas apenas agentes inativos podem ser selecionados para remoção.
6. Dentre os agentes inativos exibidos, selecione os agentes a serem removidos e clique em Excluir.

   Uma mensagem de confirmação que determina o número de agentes selecionados pergunta se você deseja continuar ou cancelar.
7. Selecione Continuar.

   Os agentes selecionados são removidos do domínio e a alteração no domínio é salva automaticamente.
8. Clique com o botão direito do mouse em Domínio e selecione Desbloquear.

Iniciar um agente

Use o método de início ou reinício do agente para o sistema operacional no host que contém o agente.

Iniciar ou reiniciar um agente em um host do Microsoft Windows

As etapas a seguir se aplicam a qualquer agente no domínio do CA Process Automation que resida em um host com um sistema operacional Windows.

Siga estas etapas:

1. Efetue logon no host do Windows em que um agente esteja instalado.
2. No menu Iniciar, selecione Programas, CA, Agente do CA Process Automation, Iniciar serviço do agente.
3. Efetue logoff do servidor.

Iniciar ou reiniciar um agente em um host do Linux

As etapas a seguir se aplicam a qualquer agente no domínio do CA Process Automation que resida em um host com um sistema operacional UNIX ou Linux.

Siga estas etapas:

1. Efetue logon no host do UNIX ou Linux em que um agente esteja instalado.
2. Altere os diretórios para:

   `usr/local/CA/PAMAgent/pamagent`
3. Execute o seguinte comando:

   `./c2oagtd.sh start`

   O agente é reiniciado.

Interromper um agente

É possível interromper um agente do CA Process Automation que está sendo executado em um host do UNIX ou Linux.

Interromper um agente em um host do Microsoft Windows

As etapas a seguir se aplicam a qualquer agente no domínio do CA Process Automation que resida em um host com um sistema operacional Windows.

Siga estas etapas:

1. Efetue logon no host do Windows em que um agente esteja instalado.
2. No menu Iniciar, selecione Programas, CA, Agente do CA Process Automation, Interromper serviço do agente.
3. Efetue logoff do servidor.

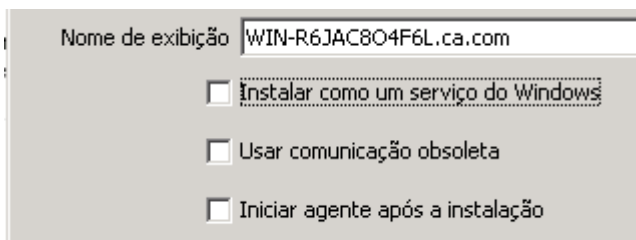
Interromper um agente em um host Linux

As etapas a seguir se aplicam a qualquer agente no domínio do CA Process Automation que resida em um host com um sistema operacional UNIX ou Linux.

Siga estas etapas:

1. Efetue logon no host do UNIX ou Linux em que um agente esteja instalado.
2. Altere os diretórios para:

   ```
   usr/local/CA/PAMAgent/pamagent
   ```

3. Execute o seguinte comando:

   ```
   ./c2oagtd.sh stop
   ```

   A execução do agente é interrompida.

Sobre a comunicação do agente

Você configura as comunicações do agente ao instalar um agente. Por padrão, os novos agentes usam a comunicação simplificada (a caixa de seleção Usar comunicação obsoleta está desmarcada).

Os agentes atualizados usam a comunicação obsoleta. É possível reconfigurar essa configuração sem reinstalar o agente.

Comunicação simplificada

A comunicação simplificada usa soquetes da web e o HTTP para produzir uma conexão persistente em uma única via, do agente para o orquestrador. O CA Process Automation usa uma porta padrão (80 ou 443) que fornece uma conexão rápida entre os componentes.

Comunicação obsoleta

A comunicação obsoleta, que usa várias portas, não é tão amigável com o firewall ou com um roteador NAT quanto a comunicação simplificada. As conexões iniciadas pelo orquestrador usadas na comunicação obsoleta não são tão eficazes quanto as conexões persistentes usadas na comunicação simplificada.

Configurar o agente para usar a comunicação simplificada

É necessário reinstalar os agentes existentes para alternar a comunicação do agente da comunicação obsoleta para a simplificada. Isto pode ser feito para todos os agentes depois de atualizar para o CA Process Automation 04.2.00 e instalar e configurar um balanceador de carga NGINX.

Reinstale cada agente conforme descrito no tópico Instalar um agente de forma interativa (na página 202). Por padrão, a caixa de seleção Usar comunicação obsoleta está desmarcada. Deixar esta caixa de seleção desmarcada, instala o agente para usar a comunicação simplificada.

O agente cria conexões de soquete da web e envia os detalhes da conexão para todos os nós do orquestrador. Os orquestradores usam a conexão de soquete da web para enviar solicitações ou atualizações para o agente, conforme necessário.

Configurar o agente para usar a comunicação obsoleta

Os agentes instalados com o CA Process Automation 4.2 usam a comunicação simplificada por padrão. Se desejar, é possível alternar a comunicação do agente de volta para a comunicação obsoleta.

Se você tiver um ambiente compatível com firewall, reconfigure o uso da porta do firewall antes de alternar da comunicação simplificada para a comunicação obsoleta. As portas Jetty usadas para a comunicação simplificada são as portas padrão 80 e 443 para HTTP e HTTPS, respectivamente. As portas tomcat usadas na comunicação obsoleta usam 8080 e 8443. Para obter mais detalhes sobre as portas do agente, consulte o tópico "Portas usadas por um Agente" no *Guia de Instalação*.

Siga estas etapas:

1. Verifique se o agente está em execução.

   Se a paleta Agentes exibir um agente do CA Process Automation como inativo, é possível iniciar o agente. Consulte o tópico Como iniciar ou interromper um agente.

2. Clique na guia Configuração e expanda Agentes, na paleta Navegador de configuração.
3. Selecione o agente para o qual deseja alternar a comunicação e clique em Bloquear.
4. Selecione a guia Propriedades para o agente selecionado.
5. Marque a caixa de seleção Usar comunicação obsoleta.
6. Selecione o agente e clique em Desbloquear.
7. Clique em Sim na caixa de diálogo Dados não salvos para salvar as alterações.

O agente encerrará a conexão de soquete da web. Depois que a conexão de soquete da web tiver sido encerrada, o agente utilizará a comunicação obsoleta.

Capítulo 9: Administrar touchpoints

Os touchpoints mapeiam nomes simbólicos para orquestradores e agentes. Os touchpoints são usados para identificar o orquestrador ou o agente em um ambiente. Uma camada é fornecida entre o CA Process Automation e a topologia da rede, permitindo que os operadores do CA Process Automation sejam configurados sem especificar explicitamente as informações do host.

A configuração de categoria de um operador especifica o touchpoint no qual executar o operador. Um usuário que está configurando um operador do CA Process Automation seleciona um nome em uma lista de touchpoints que estão configurados para executar os operadores na mesma categoria do operador referenciado. Essa inversão permite que você substitua os hosts no tempo de execução. A inversão também permite definir vários ambientes do CA Process Automation nos quais os mesmos touchpoints são mapeados para diferentes hosts reais.

Esta seção contém os seguintes tópicos:

Estratégia de implementação de touchpoint

Um *touchpoint* é uma representação lógica específica ao ambiente, de um ou mais recursos. Um *recurso gerenciado* é um agente ou orquestrador no qual os operadores de um processo são executados. Para executar um operador em um agente específico ou uma tolerância a falhas desse agente, especifique o destino como o touchpoint mapeado para eles.

Os administradores de conteúdo criam touchpoints para destinos de processo no ambiente de design depois de concluir os planos do processo, mas antes do início do processo de criação. Os criadores de conteúdo criam o processo, no qual os operadores definem como destino os touchpoints que você criou. Os criadores de conteúdo testam o processo e, em seguida, o empacotam para transição para o ambiente de produção.

Antes da transição do processo, você cria touchpoints semelhantes que associam agentes de produção ao ambiente de produção. Isto é, você cria no ambiente de produção os mesmos nomes de touchpoint ou nomes de touchpoint do proxy que usou no ambiente de criação. A criação desses touchpoints permite que os operadores no processo transicionado continuem a usar os mesmos touchpoints que o operador tem como destinos.

Considere o seguinte processo:

1. Obtenha uma versão de teste do sistema externo ou da atividade que você planeja como destino.

   Exemplos de entidades externas incluem um aplicativo da central de serviço, um banco de dados de produção ou um sistema de backup.

2. Instale um agente no host com a versão de teste da entidade planejada como destino.

   Se essa abordagem não for possível, crie uma conexão SSH de um host de agente com o host com o destino e, em seguida, crie um touchpoint do proxy.

3. Mapeie um touchpoint (ou touchpoint do proxy) para o agente no ambiente de criação que executa a cópia de teste do sistema externo de destino.

4. Os criadores executam e testam o processo em que os operadores no processo definem como destino o touchpoint para teste.

5. Durante a transição de um processo para o ambiente de produção, execute o seguinte procedimento para cada destino que seja um touchpoint de agente:

   a. Identifique um ou mais hosts que estão executando o aplicativo, banco de dados ou sistema para o destino.

   b. Instale um agente em cada host identificado.

   c. Crie um touchpoint que associe cada agente que é um destino potencial com o ambiente de produção. Nomeie o touchpoint com o mesmo nome usado no ambiente de criação.

6. Durante a transição de um processo, execute o seguinte procedimento para cada destino que seja um touchpoint do proxy:

   a. Identifique o host remoto que está executando o aplicativo, banco de dados ou sistema de destino.

   b. Instale um agente em um host disponível.

   c. Crie uma conexão SSH do host do agente com o host remoto.

   d. Crie um touchpoint do proxy que associa o host do agente ao ambiente de produção. Nomeie o touchpoint do proxy com o mesmo nome usado para o touchpoint do proxy no ambiente de criação.

Configurar touchpoints para criação e produção

Um operador que tem como destino um touchpoint pode ser executado no ambiente de criação e de produção sem alterações no campo Destino do operador. Para fazer isso, defina o mesmo nome do touchpoint em cada ambiente.

Você pode configurar os touchpoints para criação e produção quando concluir os seguintes pré-requisitos:

- Instalar agentes em hosts que o processo usará como destino no ambiente de criação.
- Instalar agentes em hosts que o processo usará como destino no ambiente de produção.

Set Up Touchpoints for Design and Production

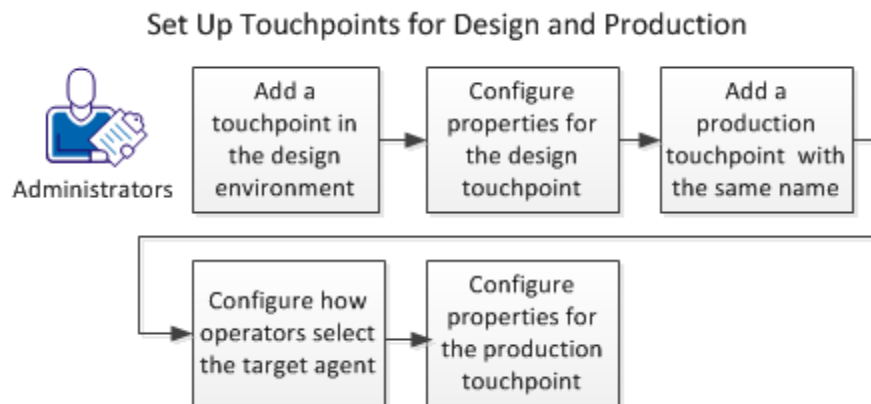
Administrators

Add a touchpoint in the design environment

Configure properties for the design touchpoint

Add a production touchpoint with the same name

Configure how operators select the target agent

Configure properties for the production touchpoint

Siga estas etapas:

1. Adicionar um touchpoint ao ambiente de criação (na página 221).
2. Configurar as propriedades do touchpoint de criação (na página 222).
3. Adicionar um touchpoint de produção com o mesmo nome (na página 223).
4. Configurar como os operadores selecionam o agente de destino (na página 224).
5. Configurar as propriedades do touchpoint de produção (na página 225).

Adicionar um touchpoint ao ambiente de criação

Um touchpoint associa um agente a um ambiente. Você pode adicionar um touchpoint e associá-lo a um agente que está instalado em um host a ser definido como destino durante a criação e o teste.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a opção Domínio no Navegador de configuração.

3. Selecione o ambiente que você usa para criação e, em seguida, clique em Bloquear.
4. Clique com o botão direito do mouse no ambiente e, em seguida, clique em Adicionar touchpoint.
5. Digite um nome para o novo touchpoint no campo Nome do touchpoint na caixa de diálogo Adicionar touchpoint: *ambiente*.
6. Selecione o agente que está instalado no host a ser definido como destino desse touchpoint.
7. Clique em Adicionar, clique em Salvar na barra de menus e, em seguida, clique com o botão direito do mouse no ambiente e selecione Desbloquear.
8. Visualize o touchpoint adicionado no nó Todos os touchpoints do ambiente de criação. Visualize a linha adicional na guia Dados do touchpoint.

Configurar as propriedades do touchpoint de criação

É possível configurar as propriedades de um touchpoint com base no ambiente. Para touchpoints associados a um ambiente de criação, você tem a opção de recuperar os operadores manualmente. Essa configuração oferece a melhor oportunidade para a solução de problemas. A segurança do touchpoint geralmente usa como destino hosts críticos à missão e não é aplicável a hosts do agente usados durante a criação.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito do mouse no ambiente com os touchpoints a configurar e, em seguida, selecione Bloquear.
3. Expanda o ambiente e, em seguida, expanda a opção Todos os touchpoints.
4. Selecione o touchpoint a configurar e, em seguida, clique na guia Propriedades.
5. Defina a propriedade Recuperação automática de operadores para permitir a recuperação de operadores manualmente. Essa configuração fornece melhor controle sobre a recuperação de operadores, quando necessário.
6. Se uma diretiva de segurança do touchpoint ativa proteger esse touchpoint, ative a propriedade Segurança do touchpoint.

   A ativação da propriedade impõe a diretiva aplicável que especifica os usuários com permissão para executar operadores no destino atual.
7. Clique em Salvar.
8. Clique com o botão direito do mouse no ambiente e, em seguida, selecione Desbloquear.

Adicionar um touchpoint de produção com o mesmo nome

Quando os criadores de conteúdo digitam nomes de touchpoints no campo Destino para operadores, o operador é executado no agente associado ao touchpoint no ambiente de criação.

O nome do touchpoint deve ser exclusivo em um ambiente. Dois ambientes podem ter touchpoints diferentes com o mesmo nome. O cenário a seguir é válido, onde existem dois touchpoints diferentes nomeados TP-125.

- O TP-125 associado ao agent-1 e ao ambiente de criação
- O TP-125 associado ao agent-2 e ao ambiente de produção

Agentes não são específicos do ambiente. Você pode associar dois touchpoints com o mesmo nome em ambientes diferentes ao mesmo agente.

Quando um processo é passado para outro ambiente, cada operador deve ser executado em um agente usado no ambiente de importação. Para se preparar para o uso de um processo importado, faça o seguinte:

1. Identifique cada touchpoint de destino de um operador em um processo que é executado no ambiente de criação. O processo pode estar na fase de planejamento ou pode estar pronto para exportação.
2. Para cada touchpoint identificado, identifique dois agentes apropriados usados no ambiente de produção nos quais o operador pode ser executado. É recomendado associar dois agentes, em vez de um, para alta disponibilidade.
3. No ambiente de produção, crie um touchpoint com o mesmo nome que o touchpoint identificado. Associe-o aos agentes apropriados usados no ambiente de produção. O procedimento a seguir descreve esta etapa.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito do mouse no ambiente de produção na paleta Navegador de configuração e, em seguida, clique em Bloquear.
3. Clique com o botão direito do mouse no ambiente de produção e, em seguida, clique em Adicionar touchpoint.
4. Digite o mesmo nome de touchpoint usado no ambiente de criação. Digite o nome no campo Nome do touchpoint na caixa de diálogo Adicionar Touchpoint: *productionEvironment*.

5. Selecione os dois agentes identificados anteriormente que podem ser usados como destino desse touchpoint.
6. Clique em Adicionar, clique em Salvar na barra de menus e, em seguida, clique com o botão direito do mouse no ambiente e selecione Desbloquear.
7. Visualize o touchpoint adicionado no nó Todos os touchpoints do ambiente de criação. Visualize a linha adicional na guia Dados do touchpoint.

Observação: se associar vários agentes ao touchpoint no ambiente de destino, você deve configurar como os operadores selecionam o agente de destino.

Mais informações:

Configurar como os operadores selecionam o agente de destino (na página 224)

Configurar como os operadores selecionam o agente de destino

Você pode associar vários agentes ao mesmo touchpoint. Quando um operador tem como destino um touchpoint, por exemplo, ele pode selecionar um agente específico ou selecionar um agente de forma aleatória. Por padrão, o operador seleciona o primeiro agente associado ao touchpoint.

É possível configurar como os operadores selecionarão o agente no qual serão executados.

- Para instruir os operadores a selecionar seu agente preferencial, atribua a prioridade 1 a esse agente. Atribua a prioridade 2 ao agente de cópia de segurança.
- Para instruir os operadores a selecionar o agente de forma aleatória, atribua a prioridade 1 a todos os agentes.

É possível configurar como os operadores selecionarão o host de destino atribuindo prioridades aos agentes associados.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o domínio, selecione o ambiente a ser configurado e clique em Bloquear.
3. Expanda o ambiente. Em Todos os touchpoints, clique no touchpoint do agente que você deseja configurar.

   A guia Agentes exibe a lista de agentes mapeados para o touchpoint selecionado. Cada agente é listado com um número de prioridade que reflete a ordem em que foi adicionado.

4. Examine as configurações de prioridade exibidas e execute uma das seguintes ações:
   - Para o balanceamento de carga, atribua o mesmo número a cada agente que possa ser o agente ativo. Por exemplo, atribua 1.
   - Para criar cópias de segurança, atribua 1 ao agente de destino com o touchpoint. Atribua 2 ao agente de cópia de segurança que assumirá a operação somente se o agente de alta prioridade ficar inativo.
   - Para ambos, atribua 1 aos agentes que participarão do balanceamento de carga e atribua um número maior aos agentes que servirão como cópias de segurança.
5. Clique em Salvar.
6. Selecione o ambiente e clique em Desbloquear.

Configurar as propriedades do touchpoint de produção

É possível configurar as propriedades de um touchpoint com base no ambiente associado. Em um ambiente de produção, ativar a opção Recuperação automática de operadores reduz o tempo necessário para restaurar a execução de um processo quando um operador com processos recuperáveis falha. A opção Segurança do touchpoint se aplica apenas aos hosts com valores altos no ambiente de produção. Portanto, defina essa propriedade se você tiver uma diretiva de segurança do touchpoint que protege os agentes associados a esse touchpoint.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito do mouse no ambiente com os touchpoints a configurar e, em seguida, selecione Bloquear.
3. Expanda o ambiente e, em seguida, expanda a opção Todos os touchpoints.
4. Selecione o touchpoint a configurar e, em seguida, clique na guia Propriedades.
5. Defina a propriedade Recuperação automática de operadores para recuperar os operadores automaticamente.

   Essa configuração reduz o impacto dos problemas de rede em usuários de produção.
6. Se os agentes de produção associados a esse touchpoint forem definidos em uma diretiva de segurança do touchpoint, ative a propriedade Segurança do touchpoint.

   A ativação da propriedade impõe a diretiva aplicável que especifica os usuários com permissão para executar operadores nesses agentes.

7. Clique em Salvar.
8. Clique com o botão direito do mouse no ambiente e, em seguida, selecione Desbloquear.

Adicionar um ou mais touchpoints

Você pode adicionar um touchpoint de cada vez.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a opção Domínio no Navegador de configuração.
3. Clique com o botão direito do mouse no ambiente a configurar e clique em Bloquear.
4. Clique com o botão direito do mouse no ambiente e, em seguida, clique em Adicionar touchpoint.
5. Digite um nome para o novo touchpoint no campo Nome do touchpoint na caixa de diálogo Adicionar touchpoint: *ambiente*.
6. Selecione um objeto a ser associado ao touchpoint na lista suspensa. Selecione:
   - Um orquestrador
   - Um agente
   - Vários agentes
7. Clique em Adicionar, clique em Salvar na barra de menus e, em seguida, clique com o botão direito do mouse no ambiente e selecione Desbloquear.
8. Exiba os touchpoints adicionados no nó Todos os touchpoints para o ambiente selecionado. Visualize a linha adicional na guia Dados do touchpoint.

Adicionar um ou mais agentes a um touchpoint existente

Você pode adicionar um ou mais agentes a um touchpoint existente. Recomendamos adicionar mais de um agente para cada touchpoint que você associar ao seu ambiente de produção. Se um agente não estiver disponível, um operador que usa como destino o touchpoint poderá ser executado em outro agente associado.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o nó Domínio na paleta Navegador de configuração, selecione um ambiente e clique em Bloquear.

3. Se um touchpoint não existir, crie um:
    a. Expanda o nó Agentes.
    b. Identifique um agente que é executado no ambiente bloqueado. Clique com o botão direito do mouse no agente e selecione Configurar touchpoint em. Em seguida, escolha o ambiente bloqueado.

       A caixa de diálogo Adicionar touchpoint do agente é exibida.
    c. Digite o nome do respectivo touchpoint e clique em OK.
4. Para adicionar um ou mais agentes a um touchpoint existente:
    a. Expanda Todos os touchpoints para o ambiente selecionado, selecione o touchpoint de destino e, em seguida, clique em Adicionar.
    b. Selecione um ou mais agentes ativos que são executados no ambiente bloqueado e clique em Adicionar. (Os agentes ativos são exibidos em verde.)

       Os novos agentes a serem associados ao touchpoint selecionado são exibidos na lista da guia Agentes.
    c. Clique em Salvar.

       O touchpoint selecionado já está associado a outros agentes.
5. Clique com o botão direito do mouse no ambiente bloqueado e selecione Desbloquear.
6. Clique em Sim no prompt para salvar as alterações.

Observação: se associar vários agentes ao touchpoint no ambiente de destino, configure como os operadores selecionam o agente de destino.

Mais informações:

Configurar como os operadores selecionam o agente de destino (na página 224)

Adicionar Touchpoints a Agentes em massa

Você pode adicionar touchpoints a novos agentes em massa, especificando os padrões para nomes de host ou endereços IP do agente. Todos os agentes com um nome do host ou endereço IP que corresponder a um padrão especificado são automaticamente configurados com um touchpoint. O nome do touchpoint é igual ao nome de exibição do agente. Um *padrão de admissão automática* é um padrão de nome de host expresso como uma expressão regular ou uma sub-rede de endereço IP expresso em anotação CIDR.

Você pode configurar diferentes padrões de admissão automática para cada ambiente ou configurar o mesmo padrão ou sobrepor padrões em diversos ambientes. Touchpoints são específicos do ambiente. Agentes não são específicos do ambiente.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a opção Domínio no Navegador de configuração.
3. Clique com o botão direito do mouse no ambiente que deseja configurar e clique em Bloquear.
4. Clique na guia Admissão automática.
5. Para cada padrão de endereço IP, execute as etapas a seguir. Em seguida, use as setas para cima e para baixo para ordenar a lista de pesquisa.
   a. Clique em Adicionar na área de Padrões do endereço IP.

      Um campo de entrada é exibido.

   b. Insira uma sub-rede IPv4 usando a anotação CIDR.

      Observação: o CA Process Automation usa a correspondência de padrões CIDR para os requisitos de auto-admit. Por exemplo, o padrão de CIDR 155.32.45.0/24 corresponde a endereços IP no intervalo 155.32.45.0 a 155.32.45.255.

6. Para cada padrão de nome de host, execute as etapas a seguir. Em seguida, use as setas para cima e para baixo para ordenar a lista de pesquisa.
   a. Clique em Adicionar na área de Padrões de nome de host.
   b. Digite um padrão de nome de host.

      Observação: o nome de host do orquestrador/agente é comparado com as expressões regulares especificadas. Por exemplo, se o padrão especificado for ca\.com$, todos os agentes/orquestradores cujos nomes de host terminarem com ca.com serão adicionados.

7. Clique com o botão direito do mouse no ambiente e clique em Desbloquear.
8. Repita esse procedimento para cada ambiente.

   O domínio procura um novo orquestrador e novos agentes com endereços IP ou nomes de host que correspondam aos padrões de admissão automática para um ou mais ambientes.

   Quando detecta esses novos agentes, o domínio cria um touchpoint para cada correspondência e o adiciona automaticamente a cada ambiente. O nome do touchpoint é o nome de exibição do agente.

   Quando detecta o orquestrador, o domínio cria um touchpoint para esse orquestrador e o adiciona ao primeiro ambiente correspondente. Um orquestrador possui apenas um touchpoint.

Exemplo de touchpoints adicionados aos ambientes com base nos padrões de admissão automática do agente

No exemplo a seguir, padrões de admissão automática sobrepostos são definidos para dois ambientes. Dois agentes são instalados, em que o endereço IP de um corresponde ao padrão de admissão automática em um ambiente e o do outro corresponde aos padrões de admissão automática em ambos os ambientes. O resultado é que três touchpoints são automaticamente adicionados.

- O Environment1 tem um padrão de auto-admit de 155.32.45.0/24 (155.32.45.0 - 155.32.45.255)
- O Environment2 tem um padrão de auto-admit de 155.32.45.32/27 (155.32.45.32 - 155.32.45.63)
- Novos agentes com esses endereços estão instalados:
  - 155.32.45.5 com o nome de exibição de host1.mycompany.com
  - 155.32.45.50 com o nome de exibição de host2.mycompany.com

Os seguintes touchpoints são automaticamente adicionados com base nos padrões de admissão automática:

- Nome do touchpoint: host1.mycompany.com no Environment1
- Nome do touchpoint: host2.mycompany.com no Environment1
- Nome do touchpoint: host2.mycompany.com no Environment2

Associar um Touchpoint a um Agente diferente

Associar um touchpoint existente a um agente diferente em casos como o seguinte:

- Um processo é regularmente executado em um host programado para a remoção da rede.

  Aqui, o touchpoint é associado a apenas um agente e esse agente está instalado em um host programado para o encerramento. Se um touchpoint estiver associado a vários agentes, nenhuma ação será necessária.

- Um processo que está sendo executado em um centro de dados agora deve ser executado em outro centro de dados.

  Aqui, o processo faz referência a um touchpoint que deve ser associado a um agente instalado em um host no novo centro de dados.

A alteração da associação do agente para um touchpoint selecionado envolve a exclusão da associação atual do agente e, em seguida, a adição de uma nova. Para executar um processo testado em vários hosts, associe o mesmo touchpoint referenciado ao agente que é executado em cada host de destino.

Você pode substituir a associação do agente para um determinado touchpoint.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a árvore para exibir Todos os touchpoints e selecione o touchpoint de destino.

   A guia Agentes no painel principal lista o(s) agente(s) atualmente associado(s) ao touchpoint selecionado.

3. Selecione o agente cuja associação deseja eliminar e clique em Excluir.
4. Quando a mensagem de confirmação da exclusão for exibida, clique em OK.

   O touchpoint do agente é removido da lista.

5. Clique em Adicionar.

   A opção Adicionar referência ao agente a: *touchpointName* é exibida com uma lista de todos os agentes. Os agentes ativos são exibidos em verde.

6. Selecione um ou mais agentes ativos e clique em Adicionar.

   O novo agente a ser associado ao touchpoint selecionado é exibido na lista da guia Agentes.

7. Clique em Salvar.

   O touchpoint selecionado já está associado a um agente diferente.

Excluir um touchpoint

Você pode excluir um touchpoint.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a opção Domínio e o ambiente com o touchpoint.
3. Clique com o botão direito do mouse no ambiente com o touchpoint e clique em Bloquear.
4. Expanda a opção Todos os touchpoints e selecione o touchpoint a ser excluído.

   A guia Agentes é aberta e lista os agentes associados ao touchpoint.
5. Selecione todos os agentes associados ao touchpoint e, em seguida, clique em Excluir.

   Uma mensagem de confirmação é exibida.
6. Clique em Sim.

   O touchpoint excluído é removido da lista Todos os touchpoints e da guia Dados do touchpoint.
7. Selecione Domínio e clique em Desbloquear.

Remover Touchpoints em massa vazios e não utilizados

A execução da remoção de agente em massa pode criar vários touchpoints vazios. Se esses touchpoints forem usados nos processos ativos, reatribua-os a outros agentes.

Você pode remover touchpoints em dois níveis:

- Para remover touchpoints selecionados em diferentes ambientes, inicie a remoção por meio do menu de clique com o botão direito Domínio.

  Você deve ter direitos de administrador de conteúdo e de domínio.
- Para remover touchpoints selecionados dentro de um ambiente, inicie a remoção por meio do menu de clique com o botão direito Ambiente.

  Você deve ter direitos de administrador de conteúdo para o ambiente selecionado para remover seus touchpoints.

Siga estas etapas:

1. Clique na guia Configuração.
2. Bloqueie o domínio ou o ambiente de destino. Se já estiver bloqueado com alterações não salvas, salve as alterações.
3. Clique com o botão direito do mouse no domínio ou ambiente de destino e selecione Remoção de touchpoint em massa.

   A caixa de diálogo Remoção de Touchpoint em massa é exibida.
4. Clique em Pesquisar ou digite uma expressão de pesquisa de nome de touchpoint e, em seguida, clique em Pesquisar.

   A lista retornada inclui apenas os nomes e estados dos touchpoints vazios correspondentes aos seus critérios de pesquisa. Se você iniciou a remoção no nível de domínio, o ambiente para cada touchpoint também é exibido.
5. Selecione os touchpoints para a exclusão na lista exibida de touchpoints que não estão mapeados para agentes e, em seguida, clique em Excluir.

   Uma confirmação detalha o número de touchpoints marcados para a exclusão.
6. Avaliar a mensagem.
   - Se o número exibido refletir o número que você pretendia selecionar, clique em Continuar para remover esses touchpoints.
   - Se tiver ocorrido um erro de seleção, clique em Cancelar e repita as etapas 4 e 5.

Renomear um Touchpoint

A renomeação de um touchpoint possui pré-requisitos somente quando o operador Executar programa ou Executar o script é executado no touchpoint.

Importante: o operador Executar programa e o operador Executar o script na categoria Execução de comando fazem referência aos touchpoints diretamente pelo nome. Portanto, atualize as referências ao touchpoint nos operadores Executar programa e Executar o script antes de renomear o touchpoint.

Siga estas etapas:

1. Clique na guia Configuração e expanda Domínio, na paleta Navegador de configuração.
2. Selecione o ambiente apropriado e, em seguida, clique em Bloquear.
3. Expanda a opção Todos os touchpoints.
4. Clique com o botão direito do mouse no touchpoint apropriado e, em seguida, clique em Renomear.

5. Digite o novo nome do touchpoint do agente.

   Observação: o ícone de dados não salvos é exibido à esquerda de sua entrada, como um lembrete para salvar as alterações. Clique em Salvar agora ou aguarde o prompt de texto.

6. Selecione o ambiente bloqueado e, em seguida, clique em Desbloquear.

   A caixa de diálogo Dados não salvos avisa para salvar as alterações.

7. Clique em Sim.

Gerenciar grupos de touchpoints

Cada touchpoint é integrante do grupo padrão chamado Todos os touchpoints. Além disso, é possível criar seus próprios grupos nomeados para agrupar os touchpoints de maneira funcional ou lógica. De maneira lógica, os grupos de touchpoints permitem que você organize os touchpoints relacionados e procure mais facilmente touchpoints em um ambiente.

De maneira funcional, os grupos de touchpoints permitem que os comandos e operadores funcionem em todos os touchpoints do grupo:

- O comando Recarregar executado em um grupo de touchpoints atualiza a lista de todos os touchpoints dentro do grupo.
- O comando Atualizar executado em um grupo de touchpoints atualiza as configurações de propriedade de todos os touchpoints do grupo.
- Um operador configurado para ser executado em um grupo no tempo de execução é executado em cada touchpoint do grupo.

Um grupo de touchpoints estará ativo se ao menos um touchpoint do grupo estiver ativo. Um grupo de touchpoints estará inativo se todos os touchpoints do grupo estiverem inativos. Se todos os touchpoints de um grupo estiverem ativos, o ícone do grupo de touchpoints será verde. Se alguns touchpoints estiverem ativos, o ícone do grupo de touchpoints será amarelo. Se todos os touchpoints de um grupo estiverem inativos, o ícone do grupo de touchpoints será vermelho.

Um usuário deve ter permissões de administrador do ambiente para criar um grupo de touchpoints em um ambiente.

Sobre grupos de touchpoints

Quando um determinado operador precisar usar vários touchpoints como destino de uma vez, os administradores criam um grupo de touchpoints que possa funcionar como destino do operador. Por exemplo:

Criar e definir como destino um grupo de touchpoints

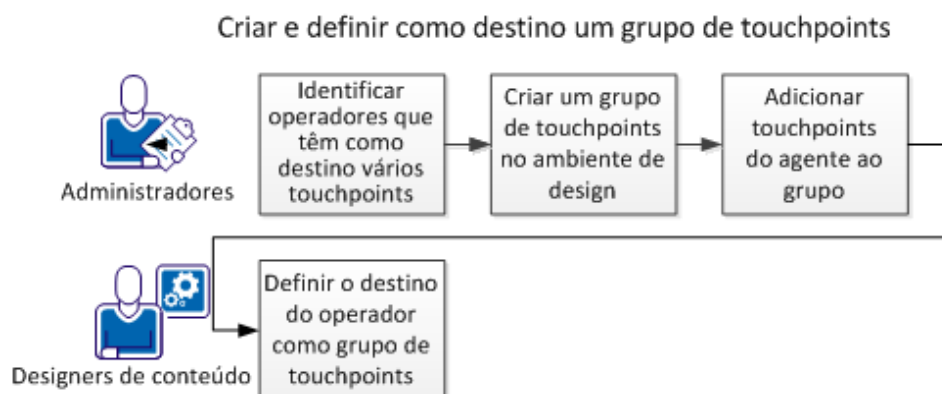
Administradores

Identificar operadores que têm como destino vários touchpoints

Criar um grupo de touchpoints no ambiente de design

Adicionar touchpoints do agente ao grupo

Designers de conteúdo

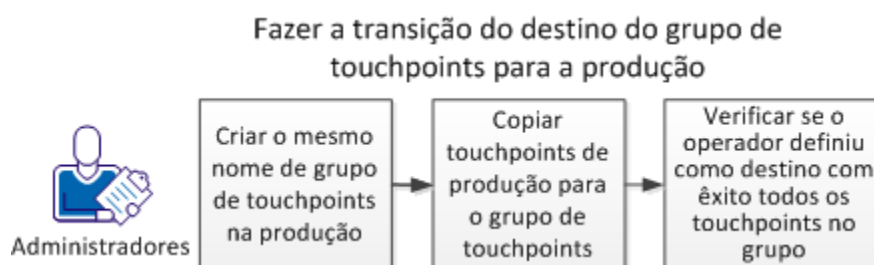
Definir o destino do operador como grupo de touchpoints

Quando os administradores fazem a transição do destino de um grupo de touchpoints para o ambiente de produção, eles criam um grupo de touchpoints no ambiente de produção. O nome do touchpoint é igual ao nome usado no ambiente de criação. Os administradores associam os orquestradores e agentes de produção ao grupo de touchpoints. Quando eles testam o processo, um dos itens que verificam é se os operadores que têm como destino um grupo de touchpoints realmente são executados em cada orquestrador ou agente representado por um touchpoint nesse grupo. Por exemplo:

Fazer a transição do destino do grupo de touchpoints para a produção

Administradores

Criar o mesmo nome de grupo de touchpoints na produção

Copiar touchpoints de produção para o grupo de touchpoints

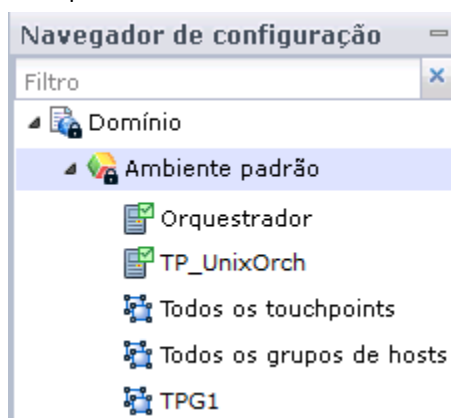
Verificar se o operador definiu como destino com êxito todos os touchpoints no grupo

Criar um grupo de touchpoints com touchpoints selecionados

Crie um grupo de touchpoints que possa funcionar como destino de um operador quando um determinado operador for obrigado a usar vários touchpoints de uma vez como destino. Você adiciona um grupo de touchpoints no nível de ambiente. Selecione cada touchpoint do grupo na hierarquia de domínio. É possível selecionar um touchpoint de orquestrador ou de agente e, em seguida, usar a opção Copiar para a fim de copiar o touchpoint selecionado para um grupo de touchpoints.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda a opção Domínio, selecione o ambiente a ser configurado e clique em Bloquear.
3. Crie um grupo de touchpoints:
   a. Clique com o botão direito do mouse em um ambiente e, em seguida, selecione Adicionar novo grupo.
   b. Na caixa de diálogo Adicionar grupo de touchpoints, digite um nome para o grupo de touchpoints e clique em OK.

      Por exemplo, se você digitou TPG1 para o nome, o novo nome do grupo aparecerá sob o ambiente selecionado, abaixo de Todos os grupos de hosts.

      Navegador de configuração
      Filtro
      Domínio
      Ambiente padrão
      Orquestrador
      TP_UnixOrch
      Todos os touchpoints
      Todos os grupos de hosts
      TPG1

   c. Clique em Salvar.

      Observação: não é possível adicionar com êxito um orquestrador a um grupo de touchpoints não salvo.

4. Copie touchpoints do orquestrador e touchpoints do agente no grupo de touchpoints. Por exemplo:

   a. Clique com o botão direito do mouse em um orquestrador e, em seguida, selecione Copiar para, *nome_do_grupo*.

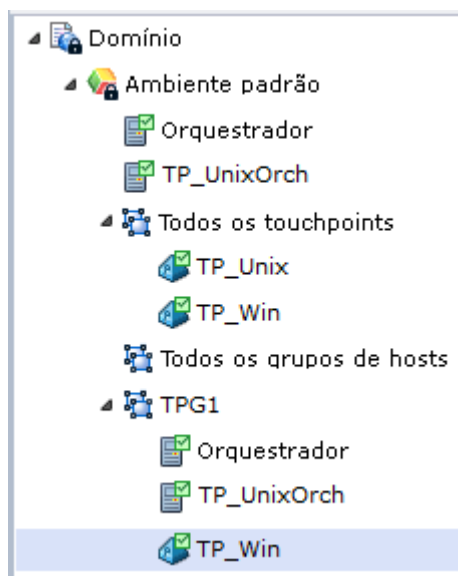
      O orquestrador selecionado aparece na hierarquia sob o nome do grupo de touchpoints selecionado.

   b. Clique em Salvar.

   c. Clique com o botão direito do mouse em outro orquestrador, selecione Copiar para e selecione o mesmo *nome_do_grupo*.

   d. Clique em Salvar.

   e. Expanda a opção Todos os touchpoints, clique com o botão direito do mouse em um touchpoint do agente, selecione Copiar para e, em seguida, selecione o mesmo *nome_do_grupo*.

   No exemplo a seguir, o grupo de touchpoints TPG1 exibe o conteúdo de dois touchpoints de orquestrador e um touchpoint de agente:

5. Selecione o ambiente e selecione Desbloquear.

   A caixa de diálogo Dados não salvos avisa para salvar as alterações.

6. Clique em Sim.

Mais informações:

Gerenciar grupos de touchpoints (na página 233)

Excluir um touchpoint de um grupo de touchpoints

A exclusão de um touchpoint de um grupo remove apenas o touchpoint desse grupo. A exclusão de um touchpoint do grupo Todos os touchpoints o remove do ambiente e de todos os grupos de touchpoints em que ele foi adicionado. Os administradores de conteúdo podem excluir um touchpoint de um grupo de touchpoints.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o domínio, selecione o ambiente a ser configurado e clique em Bloquear.
3. Expanda o grupo de touchpoints a ser configurado.
4. Selecione o touchpoint a ser removido do grupo e clique em Excluir.
5. Selecione o ambiente e clique em Desbloquear.

   A caixa de diálogo dados não salvos avisa para salvar as alterações.
6. Clique em Sim.

Excluir um grupo de touchpoints

Os administradores de conteúdo podem excluir de um ambiente um grupo de touchpoints criado pelo usuário e todos os seus touchpoints. Esse procedimento não exclui o touchpoint de qualquer outro grupo no ambiente. Não é possível excluir o grupo Todos os Touchpoints.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o domínio, selecione o ambiente a ser configurado e clique em Bloquear.
3. Clique com o botão direito do mouse no grupo de touchpoints que você deseja remover do ambiente e, em seguida, clique em Excluir.
4. Selecione o ambiente e clique em Desbloquear.

   A caixa de diálogo dados não salvos avisa para salvar as alterações.
5. Clique em Sim.

Capítulo 10: Administrar touchpoints do proxy

Quando um operador tem como destino um touchpoint do proxy, o operador é executado no host remoto para o qual o touchpoint do proxy host tem uma conexão SSH. Nenhum software de agente é instalado no host remoto. Os operadores podem ser executados em qualquer dispositivo executando o sistema operacional Windows ou UNIX. Um touchpoint do proxy sacrifica um certo desempenho, mas é útil quando o software do agente não pode ser instalado em um host de destino.

Para usar um touchpoint do proxy, você deve configurar um touchpoint do CA Process Automation para apontar para um destino remoto e criar um usuário do SSH no computador de destino.

Esta seção contém os seguintes tópicos:

Pré-requisitos do touchpoint do proxy

Os touchpoints do proxy podem ser criados configurando um touchpoint existente para ser executado como touchpoint do proxy para um computador remoto ou outro dispositivo. Um touchpoint pode ser configurado como touchpoint do proxy para um host com um ambiente operacional UNIX ou Windows. Os touchpoints do proxy usam o SSH para executar ações nos computadores de destino.

Os pré-requisitos do uso do touchpoint do proxy são os seguintes:

- O JVM (Java Virtual Machine) versão 1.6+ ou posterior é necessário no host com o touchpoint a ser configurado como touchpoint do proxy.
- Quando o destino para um touchpoint do proxy for um computador UNIX, o shell Korn (ksh) deve ser instalado no computador de destino. Se estiver ausente no destino, instale o shell Korn ou vincule-o ao shell Bash.
- Uma conta de usuário do SSH deve ser especificada no computador remoto de destino por um touchpoint do proxy.
- (Opcional) Para usar autenticação de chave pública, uma relação de confiança deve ser criada por meio do host do touchpoint do proxy para o computador remoto de destino.

  Importante: Se você executar essa etapa, siga as diretrizes documentadas nos Requisitos específicos do CA Process Automation para a conectividade de SSH.
- No CA Process Automation, o touchpoint do proxy deve ser configurado com informações de autenticação e outras especificações para o host remoto.

Requisitos específicos do CA Process Automation para a conectividade SSH

A conectividade de SSH pode ser obtida com a criação de uma conta de usuário de SSH em cada host de destino. Se você criar a relação de confiança opcional entre um host do agente e um host remoto, determinados requisitos específicos de configuração do CA Process Automation serão aplicáveis.

Quando uma solicitação a um host remoto for processada, as seguintes propriedades são lidas:

- Nome do usuário remoto.
- Senha remota.
- Caminho de chaves de SSH, se configurado.

O CA Process Automation tenta uma conexão SSH do host do agente ao host remoto especificado na solicitação. A primeira tentativa de acesso é realizada com as credenciais configuradas da conta do usuário. Se essa tentativa falhar, ocorrerá uma segunda tentativa com a autenticação baseada em chave. Para usar a autenticação de chave pública de SSH com o CA Process Automation, o nome do private key file deve corresponder ao nome da conta de usuário. Se uma senha for especificada ao serem criadas as chaves, ela deverá corresponder à senha na conta de usuário. Dessa forma, os dois campos a seguir cumprem uma função dupla.

Nome do usuário remoto

Esse é o nome de usuário da conta usada quando a autenticação for baseada nas credenciais de SSH.

Também é o nome do arquivo de chave que armazena a chave privada de SSH no caminho configurado como Caminho das chaves de SSH, quando configurado.

Senha remota

Essa é a senha da conta de usuário usada quando as credenciais de SSH forem usadas para a autenticação.

Também é a senha que será usada quando a chave pública de SSH for usada para a autenticação.

Siga essas diretrizes ao criar uma relação de confiança do host local para o host remoto:

- Digite o Nome do usuário remoto para *user_name* quando você digitar este comando:

  ```
  ssh-keygen -t dsa -b 1024 -f user_name
  ```

- Digite Senha remota como a senha.

Crie a conta de usuário de SSH no host remoto do Touchpoint do proxy

A configuração do touchpoint do proxy especifica o Nome de usuário remoto e a Senha remota da conta de usuário do SSH usada para acessar o host remoto. A conta de usuário de SSH deve ter permissões do nível de administrador, necessárias para executar os Operadores do CA Process Automation no computador de destino. Considere a possibilidade de definir a mesma conta de usuário para todos os computadores configurados de maneira semelhante que são acessados como hosts remotos. Por exemplo, adicione a conta *pamuser*, com a mesma senha, a cada host remoto.

Quando um touchpoint do proxy inicia uma conexão ao host remoto, ele cria um diretório temporário denominado c2otmp no computador de destino. Em um computador UNIX, o diretório é criado no diretório /home do usuário do SSH.

Criar uma relação de confiança de SSH para o host remoto

Se você deseja disponibilizar a autenticação da chave pública para o uso, crie uma relação de confiança do host do touchpoint do proxy para o host remoto de destino. Em seguida, teste a conectividade de SSH no computador que está executando o touchpoint do proxy para o computador de destino. Uma relação de confiança é criada entre dois computadores host.

O CA Process Automation usará a autenticação de chave pública que você configurar somente se a autenticação do usuário/senha falhar.

Para criar uma relação de confiança, use o programa ssh-keygen para gerar o par de chaves pública e privada. A chave privada permanece no host com o Agente. Copie a chave pública para o host remoto de destino que não possui Agente.

Siga estas etapas:

1. Gere um par de chaves. Use o comando a seguir, em que *user_name* é o nome de usuário na conta de usuário de SSH criada no computador de destino.

   ```
   ssh-keygen -t dsa -b 1024 -f nome_do_usuário
   ```

   Será solicitado que você forneça uma senha para uso posterior como senha.

2. Especifique a senha em resposta ao prompt.

   O arquivo de chave privada denominado *user_name* e o arquivo de chave pública denominado <user_name>.pub são criados.

3. Coloque o arquivo de chave privada denominado *user_name* em um dos seguintes locais:

   - O diretório de chaves privadas especificado na configuração do proxy.

     A chave é acessada por meio desse diretório com qualquer host para o qual não haja nenhum arquivo *target_host_name*/*user_name*.

   - O diretório SshKeys/*target_host_name*, um subdiretório do diretório de chaves privadas especificado na configuração do proxy. A chave privada é acessada por meio desse diretório quando você tenta se conectar com *user_name* a *target_host_name*.

     A opção Caminho de chaves SSH especifica o local do diretório de chaves privadas na caixa de diálogo Propriedades do touchpoint do proxy.

4. Transfira o arquivo de chave pública (*nome_de_usuário*.pub) para o host de destino e coloque-o no local onde o daemon de SSH possa encontrá-lo.

   Diferentes daemons de SSH seguem diferentes convenções. Examine as opções ssh-keygen para obter detalhes, como os requisitos de formatação para o public key file.

5. Para OpenSsh, concatene o arquivo público com o arquivo que contém as chaves autorizadas para o user_name. Execute o seguinte comando cat no host SSH de destino do proxy:

   ```
   cat user_name.pub >> ~user_name/.ssh/authorized_keys
   ```

Mais informações:

Requisitos específicos do CA Process Automation para a conectividade SSH (na página 240)

Configurar as propriedades do Touchpoint do proxy

Você pode criar um touchpoint do proxy reconfigurando um touchpoint do agente existente para ter como destino um computador remoto especificado.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o nó Domínio, selecione o ambiente a configurar e clique em Bloquear.
3. Em Todos os touchpoints, selecione o touchpoint do agente que deseja tornar um touchpoint do proxy.
4. Verifique se as seguintes propriedades estão definidas:
   - Recuperação automática dos operadores
   - Segurança do touchpoint

   Se essas propriedades não estiverem definidas, consulte o tópico Configurar propriedades do touchpoint (na página 222).
5. Marque a caixa de seleção Touchpoint do proxy.

   A seleção indica que este é um touchpoint do proxy. Um touchpoint do proxy é mapeado para um host remoto. Um host remoto normalmente não tem nenhum agente instalado.

6. Configure o host remoto e os valores para a autenticação SSH. Conclua as seguintes etapas:

   a. Digite o caminho absoluto ou relativo no host do agente em que o arquivo de chave privada está armazenado no campo Caminho de chaves SSH.

      Os nomes do arquivo de chave privada, <nome_de_usuário> e o arquivo de chave pública, <nome_de_usuário>.pub, coincidem com o nome de usuário remoto da conta de usuário.

   b. Identifique o host remoto com seu nome de domínio totalmente qualificado ou com o endereço IP no campo Host remoto.

      Observação: consulte Sintaxe de nomes de host DNS (na página 393).

   c. Digite o nome de usuário com o qual uma conexão é feita com o Daemon de SSH no host de destino no campo Nome de usuário remoto.

      A conta de usuário SSH deve ter permissões suficientes para executar tarefas administrativas no computador de destino.

   d. Digite a senha da conta de usuário associada ao nome do usuário remoto.

      Esse valor também é usado como a senha se a conectividade é estabelecida através da autenticação de chave pública SSH.

   e. Digite o número máximo de conexões simultâneas que o touchpoint do proxy pode abrir no host remoto de destino no campo Número máximo de processos ativos.

      Uma conexão de SSH permanece aberta enquanto um programa ou script é executado no host de destino. Se definido como 20 e você tentar executar 40 scripts no host remoto ao mesmo tempo, apenas 20 scripts serão executados. Os scripts que não foram iniciados aguardarão em uma fila até que os outros terminem; em seguida, eles serão iniciados.

   f. Selecione o sistema operacional do host remoto de destino.

7. Clique em Salvar.

8. Clique com o botão direito do mouse no ambiente e, em seguida, selecione Desbloquear.

Usar um Touchpoint do proxy

Quando um processo é executado, os operadores no processo executam operações em hosts de destino. Para executar um operador em um host remoto que não possui agente, primeiro crie uma conexão SSH de um host do agente para o host remoto. Quando você cria um touchpoint e seleciona um agente com uma conexão com um host remoto, esse touchpoint torna-se um touchpoint do proxy. Quando um operador especifica um touchpoint do proxy como o destino, a operação afeta o host remoto.

Para executar uma operação em vários touchpoints do proxy configurados de maneira semelhante, você pode agrupá-los em um grupo de touchpoints. Em seguida, especifique o grupo de touchpoints como o destino ao configurar as propriedades do operador. No tempo de execução, o operador é executado em todos os touchpoints do proxy do grupo.

Mais informações:

Gerenciar grupos de touchpoints (na página 233)

Capítulo 11: Administrar grupos de hosts

O CA Process Automation pode executar operadores em um destino que não possui agente ou touchpoint quando você referenciar esse destino em um grupo de hosts. Os designers de conteúdo podem especificar um destino por seu endereço IP ou nome de domínio totalmente qualificado (FQDN).

Observação: consulte Sintaxe de nomes de host DNS (na página 393).

Quando o mesmo grupo de hosts reside em vários agentes, o agente selecionado para executar o operador depende da prioridade do agente.

Esta seção contém os seguintes tópicos:

Sobre Grupos de hosts

Um *grupo de hosts* representa um grupo de hosts, normalmente com nomes ou endereços IP semelhantes, cada um dos quais podendo ser especificado em um operador com seu endereço IP ou FQDN. Um grupo de hosts referencia os hosts como sub-redes de endereços IP, padrões de nome de host ou uma lista de endereços IP e FQDNs específicos.

Grupos de hosts fornecem acesso direto, ou seja, a capacidade de especificar um endereço IP ou FQDN em um operador, em oposição a um nome de touchpoint ou touchpoint do proxy. Os hosts referenciados em um grupo de hosts não precisam de associações a agentes ou touchpoints do proxy. Evite incluir um host que pertença a um orquestrador agrupado em um grupo de hosts. Os designers de conteúdo não podem ser o destino desse host pelo endereço IP ou FQDN.

Você pode definir vários grupos de hosts no mesmo agente. Um determinado agente pode ter um grupo de hosts para variantes de um sistema operacional Windows e outro para as do UNIX.

É possível definir o mesmo grupo de hosts em um ou mais agentes. Quando o mesmo grupo de hosts reside em vários agentes, o agente selecionado para executar o operador depende da prioridade do agente.

Para executar os operadores do CA Process Automation em um host remoto, um host local com um agente do CA Process Automation mapeado para um grupo de hosts deve obter acesso ao host de destino. O agente usa o SSH para obter acesso a um host remoto de destino e executar os operadores nele. Você define o acesso ao SSH por meio do host do agente para cada host de destino representado pelo grupo de hosts com uma conta de usuário do SSH e, opcionalmente, uma relação de confiança de SSH.

As propriedades de um grupo de hosts incluem uma configuração do número máximo de conexões SSH. Os servidores SSHD geralmente têm limites nas configurações padrão. A conexão SSH permanece aberta enquanto o programa ou script está em execução no host de destino. O CA Process Automation implementa o enfileiramento interno por destino. Se você definir o valor como 20 e executar 40 scripts ao mesmo tempo no mesmo host de destino, apenas 20 serão executados simultaneamente. Os novos scripts iniciam à medida que os outros terminam. Com grupos de hosts, em que o mesmo agente é um proxy para vários hosts remotos, cada host remoto tem um limite específico. Dessa forma, essa configuração não afeta o número de hosts no grupo de hosts. O limite para o número de hosts é o número máximo de conexões TCP simultâneas que o sistema operacional para o agente suporta. Alguns sistemas operacionais aceitam um grande número de conexões TCP.

Importante: Embora um grupo de hosts possa incluir hosts remotos com agentes, não crie um grupo de hosts com agentes como um meio de permitir que eles sejam referenciados diretamente. A referência por touchpoint e touchpoint do proxy é altamente preferencial pela sua flexibilidade e velocidade de processamento.

Processo de implementação de grupo de hosts

Você pode configurar um grupo de hosts em qualquer agente existente. Um agente não precisa ser configurado como um touchpoint para hospedar um grupo de hosts. O host do agente do grupo de hosts usa o SSH para acessar e executar ações em um host remoto. Parte da preparação do grupo de hosts é ativar a autenticação de SSH. Quando os criadores de conteúdo têm como destino um integrante de um grupo de hosts em uma definição de operador, eles referenciam o host de destino pelo seu endereço IP ou FQDN.

Prepare-se para usar um grupo de hosts executando as tarefas e procedimentos a seguir. Os tópicos que fornecem detalhes sobre os procedimentos seguem esta visão geral do processo.

1. Criar um grupo de hosts. (na página 250)
2. Configurar as propriedades do grupo de hosts (na página 251). Ou seja, especifique os valores para todas as configurações, com exceção das chaves de SSH.
   - Para obter ajuda ao inserir padrões, consulte Como definir os padrões de nome do host remoto usando expressões regulares. (na página 253)
   - (Opcional) Para a autenticação de chave pública, configure o Caminho de chaves SSH.

     Observação: o CA Process Automation obterá acesso com autenticação de chave pública somente quando o acesso falhar com as credenciais da conta de usuário.
3. No host do agente do grupo de hosts, verifique se o JVM (Java Virtual Machine) versão 1.7 ou 1.6 (não posterior à versão 1.6.0_45) está instalado. O JVM vem com o JRE ou JDK. O JVM de 32 e 64 bits é suportado para os agentes instalados nos hosts com sistemas operacionais Windows. Use o seguinte comando para verificar se a versão Java é uma versão válida. A seguir, um exemplo:

   ```
   Versão Java
   ```

   Exemplo de resposta:

   ```
   Java versão "1.6.0_x", uma versão válida
   ```
4. Crie credenciais de SSH em hosts em um grupo de hosts (na página 256). Defina uma conta de usuário com as credenciais de SSH especificadas nas propriedades do grupo de hosts para Nome de usuário remoto e Senha remota.
5. Em cada host UNIX remoto ao qual o grupo de hosts faz referência, verifique se o shell Korn está instalado. Se o shell Korn não estiver instalado, execute uma das seguintes ações:
   - Instale o shell Korn.
   - Crie um link de software a partir de um shell Bash existente para o shell Korn usando o local retornado. Por exemplo:

   ```
   Em –s  /bin/bash /bin/ksh
   ```

6. Siga as seguintes etapas para concluir a configuração da autenticação de chave pública. Estas etapas se aplicam a uma especificação de Caminho de chaves SSH.

   ■ Verifique se o caminho digitado para o Caminho de chaves SSH na configuração do grupo de hosts existe no host do agente. Se não existir, crie-o. Por exemplo:

     Windows: C:\PAM\Sshkeys

     UNIX: /home/PAM/Sshkeys

   ■ Verifique se você possui o utilitário ssh-keygen ou baixe-o. Em um sistema Windows, o ssh-keygen.exe aparece no diretório C:\Arquivos de Programas\OpenSSH\bin. O diretório bin também contém outros arquivos que permitem usar os comandos do UNIX.

     Use este utilitário para gerar o par de chaves pública/privada.

   ■ Verifique se você pode copiar um arquivo de um host para outro. Se necessário, faça download de um utilitário de cópia como scp ou Winscp.

     Copie a chave pública do host do agente para cada host remoto.

   ■ Crie o diretório de destino e o arquivo de destino para a chave pública. (na página 257)

   ■ Criar uma relação de confiança para um host remoto referenciado por um grupo de hosts (na página 258).

     Importante: Siga estas instruções cuidadosamente. Essas etapas incluem os requisitos específicos do CA Process Automation, que variam desde a implementação padrão dos pares de chaves DSA.

Mais informações:

Requisitos específicos do CA Process Automation para a conectividade SSH (na página 240)

Criar um Grupo de hosts

Você pode adicionar um grupo de hosts a um ambiente selecionado e, em seguida, selecionar o agente. Ou, pode configurar um grupo de hosts em um agente e, em seguida, selecionar o ambiente. A combinação do nome do agente e o nome do grupo de hosts deve ser exclusiva em um ambiente.

Siga estas etapas:

1. Clique na guia Configuração.
2. Selecione o ambiente a ser configurado e clique em Bloquear.

3. Para adicionar um grupo de hosts a um ambiente selecionado, siga estas etapas:

   a. Clique com o botão direito do mouse no ambiente bloqueado e, em seguida, selecione Adicionar grupo de hosts.

      O ambiente *Adicionar grupo de hosts* é exibido.

   b. Digite o nome do grupo de hosts.

   c. Selecione um agente em exibição e, em seguida, clique em Adicionar.

4. Para adicionar um grupo de hosts a um agente selecionado, siga estas etapas:

   a. Expanda o nó Agentes.

   b. Clique com o botão direito do mouse no agente desejado, selecione Configurar grupo de hosts em e selecione o ambiente desejado.

      A caixa de diálogo Adicionar grupo de hosts do agente é exibida.

   c. Digite o nome do grupo de hosts no campo Nome do grupo de hosts e clique em OK.

      Se você digitar o nome de um grupo de hosts existente, o agente selecionado será mapeado para esse grupo.

5. Exiba o nome do grupo de hosts da seguinte maneira:

   ■ Expanda o nó Todos os grupos de hosts para o ambiente onde criou o grupo de hosts.

   ■ Expanda a opção Agentes e selecione o agente com o grupo de hosts. O novo grupo de hosts é listado na guia Grupos de hosts e touchpoints associados com o caminho de hierarquia de domínio.

Mais informações:

Processo de implementação de grupo de hosts (na página 249)

Configurar propriedades do Grupo de hosts

É possível configurar as propriedades de um grupo de hosts na guia Configuração. Você estabelece conectividade entre o agente e cada host remoto no grupo de hosts com produtos de terceiros.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda o Domínio.
3. Expanda o ambiente com o grupo de hosts.
4. Expanda Todos os grupos de hosts.

5. Selecione o grupo de hosts a configurar e, em seguida, clique na guia Propriedades.
6. Defina as propriedades do grupo de hosts selecionado.
    a. Defina Recuperação automática de operadores e Segurança do touchpoint como necessário ou aceite o padrão, a opção Herdar do ambiente.
    b. Para Caminho de chaves SSH, indique o caminho de destino que você criou no agente para armazenar o arquivo de chave privada.

        Se o host do agente tiver um sistema operacional Windows, digite: `C:\PAM\SshKeys`

        Se o host do agente tiver um sistema operacional UNIX ou Linux, digite: `/home/PAM/Sshkeys`

        Importante: Crie o caminho de destino no host do agente.
    c. Para cada padrão de nome de host remoto, clique no botão Adicionar parâmetro e defina um padrão de nome de host.

        Consulte o tópico Como definir os padrões de nome de host remoto usando expressões regulares (na página 253).
    d. Digite as credenciais da conta de usuário que você criou ou pretende criar em cada host remoto referenciado por esse grupo de hosts.

        Observação: se você configurar a autenticação de chave pública, esse valor deverá ser especificado como *nome-de-usuário* no comando para gerar os arquivos de chave. Se estiver usando a autenticação de chave pública com uma frase secreta, digite a frase secreta em Senha remota.
    e. Preencha os campos intuitivos restantes.
7. Clique em Salvar.
8. Clique com o botão direito do mouse no ambiente bloqueado e selecione Desbloquear.

    A configuração de propriedades faz parte da configuração total. Você deve criar uma conta de usuário em cada host remoto com as credenciais configuradas aqui. Isso fornece o acesso de SSH do agente para cada host remoto no grupo de hosts. Estabelecer uma relação de confiança com chaves públicas e privadas é opcional.

Mais informações:

Processo de implementação de grupo de hosts (na página 249)

Como definir os padrões de nome de host remoto usando expressões regulares

Quando você configurar grupos de hosts, especifique os padrões de nome de host e endereço IP ou ambos. Operadores de expressão regular que você pode aplicar ao definir padrões de host remoto para os Grupos de hosts:

- ^ (acento circunflexo) significa que começa com.
- \ (esc) significa interpretar o caractere do operador que segue imediatamente como um literal.
- . (ponto) dentro de uma expressão significa qualquer caractere. A expressão a.b corresponde a qualquer sequência de três caracteres começando com “a” e terminando com “b”.
- .* (ponto asterisco) significa aceitar qualquer caractere qualquer número de vezes. A expressão a.*b corresponde a uma cadeia de caracteres de qualquer tamanho começando com "a" e terminando com "b".
- $ (cifrão) significa que termina com.

Considere a expressão regular como uma maneira de não expressar nada no FQDN, incluindo:

- um padrão inicial (^String)
- um padrão intermediário (String)
- uma padrão final (String$)
- um padrão preciso (^stringcompontosesc$)

A tabela a seguir contém exemplos projetados para ajudá-lo a digitar padrões de nomes de hosts de uma forma que ajude a garantir o processamento eficiente. Se você digitar um FQDN ou subdomínio sem operadores, o FQDN ou grupo que você deseja mapear será encontrado, mas o processamento não será tão eficaz. Como prática recomendada, inclua as seguintes combinações de expressão regular nos padrões de nome de host digitados para os Padrões de host remoto.

Combinações comuns	Descrição	Exemplo de FQDN e de Grupo de hosts
^<hostname>	O acento circunflexo como primeiro caractere significa que o padrão começa com o texto que o segue.	**FQDN:** ^host1\.ca\.com$ corresponde apenas a host1.ca.com (Porém, host1\.ca\.com$ sem o acento circunflexo precedente pesquisa cada host com um nome que termine com host1.ca.com, como aaaahost1.ca.com) **Grupo:** ca\.com$ sem o acento circunflexo precedente corresponde a cada FQDN no subdomínio ca.com.

Combinações comuns	Descrição	Exemplo de FQDN e de Grupo de hosts
\.	A combinação esc/ponto (\.) significa interpretar o ponto como um literal.	**FQDN:** ^host1\.ca\.com$ corresponde apenas a host1.ca.com (Porém, ^host.ca.com$ sem um esc antes de cada ponto pode corresponder a: host1Mca0com) **Grupo:** ^host.\.ca\.com$ com um ponto depois do host pode corresponder a hosts denominados {host0, host1, ...hostZ} no domínio ca.com.
.*<domain>	A combinação ponto/asterisco (.*) permite que tudo corresponda.	**Grupo:** .*\.ca\.com$, um domínio precedido por . * corresponde a todos os hosts do Domínio.
<domain name>$	O cifrão após um nome de domínio significa que o padrão termina com o domínio especificado.	**FQDN:** ^host1\.ca\.com$ corresponde apenas a host1.ca.com (Porém, ^ host1\ .ca\ .com sem o operador $ final pode corresponder a: host1,ca.comaaaaaaa)

Exemplos

Padrões do endereço IP remoto

Especifica qualquer combinação do seguinte, onde os endereços IP são estáticos, em vez de dinâmicos. Clique em Adicionar para criar cada linha.

- Uma lista de endereços IP IPv4.
- Uma ou mais sub-redes IPv4 usando a notação CIDR.

Padrões do nome do host remoto

Especifica um grupo de hosts remotos com uma lista de nomes de domínio totalmente qualificados (FQDN) ou padrões de expressão regular para um subdomínio. Selecione Adicionar para criar uma linha para cada entrada de padrão.

Por exemplo:

- abc\.mycompany\.com
- .*pam-lnx\.mycompany\.com$

  Esse padrão corresponde a qualquer nome de host que termine com pam-lnx no domínio da sua empresa, em que mycompany é substituído pelo nome da sua empresa.

- ^machine1\.mycompany\.com$

  Especificamente, ^machine1\.mycompany\.com$ expressa um Nome de domínio totalmente qualificado (FQDN) como uma expressão regular. Esse padrão corresponde apenas ao FQDN que atende a todos estes critérios:

  começa com *machine1.*

  termina com *com.*

  contém *machine1*, depois *dot*, depois *mycompany*, depois *dot* e, em seguida, *com*.

Criar credenciais de SSH em hosts em um grupo de hosts

Uma configuração do grupo de hosts especifica as credenciais de SSH da seguinte maneira.

- Nome do usuário remoto
- Senha remota

Efetue logon em cada host ao qual o grupo de hosts faz referência. Crie uma conta de usuário com essas credenciais de SSH. Essa conta de usuário de SSH deve ter permissões suficientes para as seguintes tarefas:

- Executar tarefas administrativas.
- Executar operadores do CA Process Automation em cada computador de destino.

O agente usa o nome de usuário da conta de usuário do SSH para se conectar ao Daemon de SSH no host remoto de destino. O host de destino pode ser qualquer host que corresponda aos Padrões de nome de host remoto ou aos Padrões de endereço IP remoto na configuração do grupo de hosts.

O host do agente do grupo de hosts inicia uma conexão com o host remoto, como se segue:

1. Efetua logon no host remoto com as credenciais especificadas.
2. Cria um diretório temporário denominado c2otmp.

   Esse diretório será criado no diretório /home do usuário de SSH, se o host de destino for um computador UNIX. Por exemplo:

   ```
   /home/<nome_do_usuário>/c20tmp
   ```

Mais informações:

Processo de implementação de grupo de hosts (na página 249)

Criar o diretório e o arquivo de destino para a chave pública

Se decidir criar relações de confiança opcionais para hosts remotos referenciados pelo grupo de hosts, primeiro verifique a existência do seguinte diretório e arquivo em cada host remoto. Se o diretório ou o arquivo não existir, crie-o.

O seguinte é necessário em cada host remoto antes de criar a relação de confiança do host com o grupo de hosts.

- O diretório .ssh sob /home/<user_name>, o diretório de destino para o <user_name>.pub
- Um arquivo authorized_keys, para qual a chave pública contidas em <user_name>.pub pode ser acrescentado. O ~/.ssh/authorized_keys é o arquivo padrão que lista as chaves públicas que são permitidas para a autenticação DSA.

É possível criar o diretório .ssh e o arquivo authorized_keys em um host remoto UNIX ou Linux

Siga estas etapas:

1. Use o SSH para acessar um host remoto e efetuar logon com o Nome de usuário remoto e a Senha remota configurada para o grupo de hosts.
2. Verifique se o diretório atual é seu diretório inicial. Digite:

   pwd

   A resposta é:

   `/home/`*`nome_do_usuário`*
3. Crie o diretório .ssh neste caminho e navegue para o novo diretório.

   ```
   mkdir .ssh
   cd .ssh
   ```
4. Crie authorized_keys no diretório .ssh.

   ```
   cat > authorized_keys
   ```

   Um arquivo authorized_keys vazio é criado no diretório /home/*nome_do_usuário*/.ssh.

Para criar o diretório .ssh e o arquivo authorized_keys em um servidor Windows do host remoto

1. Use a área de trabalho remota para acessar o host remoto e efetuar logon com o Nome de usuário remoto e a Senha remota configurada para o grupo de hosts.
2. Navegue até a sua pasta inicial. Por exemplo,\Users*nome_do_usuário*.
3. Se uma pasta named.ssh não existir, crie uma nova pasta e nomeie-a como .ssh.
4. Na pasta a seguir, crie um arquivo chamado authorized_keys com nenhuma extensão.

\Users*nome_do_usuário*\.ssh

O seguinte arquivo vazio é criado.

\Users*nome_do_usuário*\.ssh\authorized_keys

Criar uma relação de confiança para um host remoto referenciado por um Grupo de hosts

Um *host remoto* é aquele referenciado por um grupo de hosts. O grupo de hosts é configurado em um host com um agente; e o host remoto normalmente não tem agentes. Para usar um host remoto como destino, é necessário que um operador de processo tenha conectividade SSH entre um host do agente e o host remoto referenciado.

Estabeleça uma conexão SSH com um dos seguintes métodos:

- Criar uma relação de confiança entre o host do agente e o host remoto. Esse método cria um par de chaves pública/privada.
- Criar uma conta de usuário no host remoto. Esse método cria credenciais.

Quando você cria uma conta de usuário *e* uma relação de confiança, o produto usa a relação de confiança como o mecanismo de backup. Se a autenticação falhar para as credenciais configuradas, o produto fará a autenticação com o par de chaves.

Gere um par de chaves com o programa SSH-keygen. Salve a chave privada no Caminho de chaves SSH configurado e, em seguida, copie a chave pública em cada host remoto referenciado pelo grupo de hosts. Coloque o arquivo de chave pública onde o daemon de SSH possa encontrá-lo. O daemon de OpenSSH, sshd, procura a chave em /home/*nome_do_usuário*/.ssh/authorized_keys.

Você pode criar uma relação de confiança com um host remoto referenciado por um grupo de hosts.

Siga estas etapas:

1. Efetue logon no host que contém o agente onde o grupo de hosts está definido.
2. Abra um prompt de comando e altere os diretórios para um caminho a partir do qual gerar o par de chaves.

   Por exemplo, se você fez download do OpenSSH em um sistema Windows, altere para o diretório C:\Arquivos de Programas\OpenSSH\bin que contém o programa ssh-keygen.

3. Gere um par de chaves com o seguinte comando:

   `ssh-keygen -t dsa -b 1024 -f` *`nome_do_usuário`*

   nome_do_usuário

   Define o valor que você configurou como Nome de usuário remoto no Grupo de hosts.

   A mensagem e o prompt a seguir são exibidos:

   `Gerando par de chaves pública/privada de DSA.`

   `Digite a senha <empty for no passphrase>:`

4. Digite o valor que você configurou como Senha remota no Grupo de hosts. Esse valor é obrigatório.

   O prompt a seguir é exibido:

   `Digite a mesma senha novamente:`

5. Digite o valor de Senha remota novamente.

   As mensagens a seguir são exibidas:

   `Sua identificação foi salva em` *`nome_do_usuário`*`.`

   `Seu arquivo de chave pública foi salvo em` *`nome_do_usuário`*`.pub.`

   `A impressão digital da chave é:`

   `fingerprint_string login_name@nome_do_host`

   O produto cria o arquivo de chave privada denominado *nome_do_usuário* e o arquivo de chave pública denominado *nome_do_usuário* .pub. A frase secreta do arquivo de chave é igual à senha da conta de usuário utilizada para o acesso de SSH.

6. Mova o arquivo de chave privada denominado *nome_do_usuário* para o local configurado como Caminho de chaves SSH do grupo de hosts. Por exemplo:

   - **Windows:** C:\PAM\Sshkeys
   - **UNIX:** /home/PAM/Sshkeys

7. Transfira o arquivo de chave pública *(nome_do_usuário*.pub) para cada host referenciado pelo grupo de hosts e coloque-o onde o daemon de SSH possa encontrá-lo.

   Diferentes daemons de SSH seguem diferentes convenções. Examine as opções de ssh-keygen para obter os requisitos de formatação do arquivo de chave pública.

8. Para OpenSsh, anexe a chave pública contida em *nome_do_usuário*.pub ao arquivo que contém todas as chaves autorizadas utilizadas pelo host. O daemon de SSH OpenSSH (sshd) pesquisa o arquivo authorized_keys. O arquivo authorized_keys deve estar no diretório .ssh no caminho do diretório principal.

   a. Execute o seguinte comando em cada host referenciado pelo grupo de hosts:

      ```
      cat nome_do_usuário.pub >>
      home/user_name/.ssh/authorized_keys
      ```

   b. Alterne os usuários para a raiz e reinicie o serviço de ssh:

      ```
      su root
      ```

      ```
      reinicialização do sshd de serviço
      ```

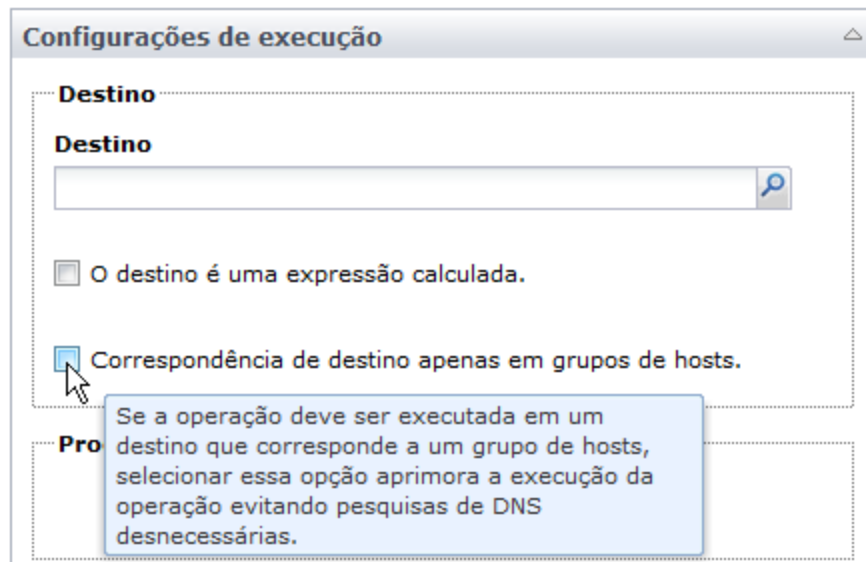
9. Verifique se o acesso foi estabelecido. Efetue logon no host com o agente e ssh para o host remoto. Se o logon for bem-sucedido, a relação de confiança será estabelecida. Digite o comando a seguir no host do agente:

   ```
   ssh nome_do_usuário@host_remoto
   ```

Garantir o processamento eficiente de referências de grupo de hosts

Este tópico, que é relevante para os criadores de conteúdo, aborda informações de administrador.

Durante a criação do processo, os criadores de conteúdo especificam as configurações de execução para cada operador. O exemplo a seguir mostra uma caixa de diálogo parcial com o campo Destino e a caixa de seleção Fazer correspondência do destino apenas em grupos de hosts.

Configurações de execução
Destino
Destino
O destino é uma expressão calculada.
Correspondência de destino apenas em grupos de hosts.
Pro
Se a operação deve ser executada em um destino que corresponde a um grupo de hosts, selecionar essa opção aprimora a execução da operação evitando pesquisas de DNS desnecessárias.

Quando o campo Destino contiver um nome do touchpoint, um nome do touchpoint do proxy, ou uma ID do agente, desmarque a caixa de seleção Fazer correspondência do destino apenas em grupos de hosts.

Quando o campo Destino contiver um endereço IP de um host específico, selecione Fazer correspondência do destino apenas em grupos de hosts. A especificação de um endereço IP ou de um nome de host no campo Destino é válida somente se um grupo de hosts no ambiente atual fizer referência ao host correspondente.

Importante: se um processo for destinado para exportação em uma pasta como pacote de conteúdo, não digite um endereço IP no campo Destino. Em vez disso, digite o nome do conjunto de dados que contém o endereço IP. Além disso:

- Selecione a opção O destino é uma expressão calculada.
- Selecione a opção Fazer correspondência do destino apenas em grupos de hosts. Um conjunto de dados que faz referência a um endereço IP é válido se um grupo de hosts no ambiente atual fizer referência ao host correspondente.

Para compreender a finalidade dessa caixa de seleção, considere o caso em que:

- O campo Destino contém a entrada *algum_host*, onde a entrada é o nome de um host em um grupo de hosts.
- A caixa de seleção Fazer correspondência do destino apenas em grupos de hosts está desmarcada.

O processamento de tempo de execução avalia e processa a entrada de Destino na seguinte sequência:

1. Se a entrada for o nome de um touchpoint, é executada no host com o agente associado ao touchpoint.
2. Se a entrada for um nome de touchpoint do proxy, é executada no host com a conexão SSH com o agente associado ao touchpoint do proxy.
3. Se a entrada for uma ID do agente, é executada no host com essa ID do agente.
4. Se a entrada for um endereço IP ou um nome do host ao qual um grupo de hosts faz referência, é executada nesse host.

   Observação: o operador falhará se você marcar a caixa de seleção Fazer correspondência do destino apenas em grupos de hosts quando o destino especificado *não* fizer parte de um grupo de hosts. O operador falhará mesmo que o destino seja um nome do touchpoint, um nome do touchpoint do proxy ou uma ID do agente válida.

Quando evitar usar referências de grupo de hosts como destinos

Quando um processo é exportado em uma pasta como pacote de conteúdo:

- Os processos *não* podem ser modificados no ambiente de importação.
- Os conjuntos de dados *podem* ser modificados no ambiente de importação.

Se o campo Destino de um operador contiver um endereço IP ou nome do host, o processo importado não poderá ser executado com êxito. A entrada Destino do operador não pode ser modificada no ambiente de importação.

A recomendação para conteúdo redistribuível é usar conjuntos de dados para os parâmetros de configuração. O criador de conteúdo cria uma variável do conjunto de dados que armazena um endereço IP. Em seguida, o criador de conteúdo digita essa variável do conjunto de dados no campo Destino do operador. Um administrador no ambiente de importação pode atualizar o conjunto de dados com um valor de endereço IP ao qual um grupo de hosts no ambiente de importação faz referência.

Como os grupos de hosts se comparam aos touchpoints do proxy

Grupos de hosts e touchpoints do proxy são semelhantes das seguintes maneiras:

- Ambos executam em agentes.
- Ambos acessam hosts remotos por meio do SSH.
- Ambos oferecem suporte para os mesmos operadores do CA Process Automation que podem ser executados em hosts remotos por meio do SSH.
- As categorias configuradas para os operadores exigidos devem estar em execução no host do agente no qual o grupo de hosts ou touchpoints do proxy está configurado.

Os grupos de hosts diferem dos touchpoints do proxy das seguintes maneiras:

- A relação entre um grupo de hosts e possíveis hosts de destino é de um para muitos, enquanto a entre um touchpoint do proxy e o host de destino é de um para um.
- Os criadores de conteúdo podem usar como destino vários hosts com touchpoints do proxy associados, especificando um grupo de touchpoints. Os criadores de conteúdo não podem usar como destino vários hosts que tenham apenas uma referência de grupo de hosts.
- Os criadores de conteúdo especificam o host remoto como um destino pelo seu nome de touchpoint, quando o host remoto tiver um touchpoint do proxy associado. Os criadores de conteúdo especificam o host remoto como um destino por seu endereço IP ou FQDN quando o host remoto tiver uma referência de grupo de hosts.

Capítulo 12: Administrar categorias do operador e grupos do operador personalizado

Este capítulo descreve conceitos e procedimentos relevantes para configurar as configurações padrão comuns para operadores em nível de categoria. Também aborda como configurar os valores das variáveis que podem ser definidas para os grupos de operadores personalizados.

Observação: não é necessário configurar módulos (categorias do operador). A prática recomendada é que o criador de conteúdo crie conjuntos de dados globais para as configurações de módulo. Em seguida, o criador de conteúdo usa expressões que fazem referência a variáveis do conjunto de dados nas propriedades do operador.

Esta seção contém os seguintes tópicos:

Categorias do operador e pastas do operador

As categorias do operador correspondem às pastas do operador. Os administradores configuram as categorias do operador na guia Módulos, começando no nível Domínio. Os criadores de conteúdo expandem as pastas do operador para exibir um grupo de operadores na categoria indicada. A paleta Operadores na guia Criador exibe pastas do operador.

Clique na guia Configuração, selecione Domínio e clique na guia Módulos para listar as categorias de operador em Nome.

Observação: a lista Nome também pode incluir grupos publicados que são criados para operadores personalizados. Os designers de conteúdo podem expandir essas pastas do grupo para exibir um grupo de operadores personalizados no grupo de configuração nomeado. As pastas do grupo de configuração que são exibidas aqui para operadores personalizados também são exibidas na paleta Operadores da guia Criador.

Conteúdo de "Domínio"

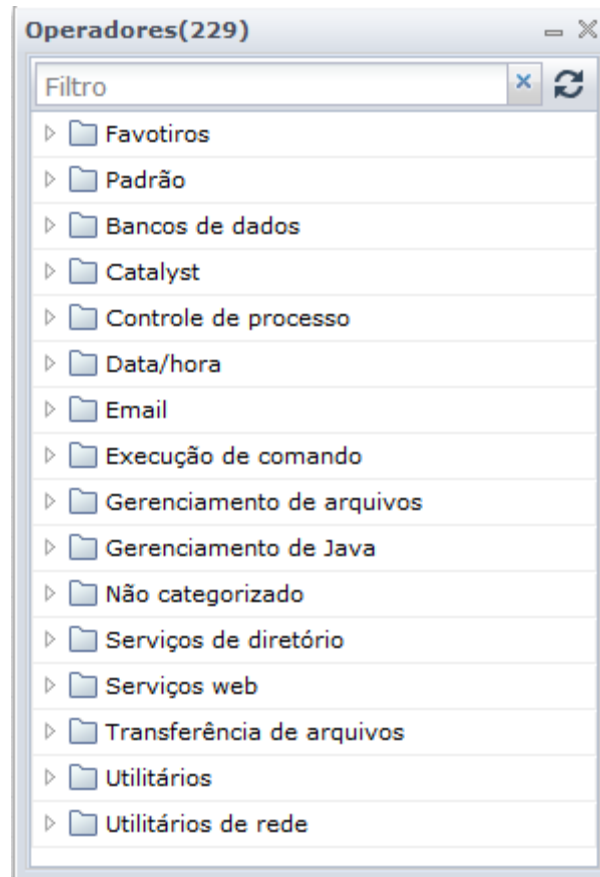
Segurança | Propriedades | Módulos | Disparadores | Trilhas de audit...

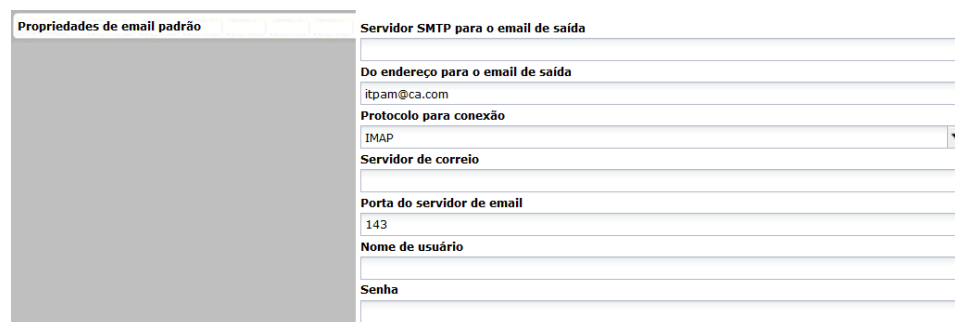
Nome	Descrição
Bancos de dados	Este é o módulo de bancos de dados para se comunicar com vários servidores do banco de dados
Catalyst	Fornece acesso aos conectores do Catalyst
Controle de processo	Executa, monitora e controla os processos do CA Process Automation.
Data/hora	Executa restrições de hora e calendário nos processos do CA Process Automation.
Email	Este é o serviço de email que lê emails a partir do servidor usando protocolos IMAP/POP3.
Execução de comando	Executa programas e scripts no ambiente operacional do host.
Gerenciamento de arquivos	Este módulo monitora diretórios e arquivos, bem como seus conteúdos
Gerenciamento de Java	Fornece uma interface de gerenciamento para sistemas externo que ofereçam suporte a JMX.
Serviços de diretório	Fornece uma interface para suporte a LDAP/AD.
Serviços web	Fornece uma interface de serviços externos expostos pelo SOAP.
Transferência de arquivos	Fornece as operações de transferência de arquivo (FTP/SFTP).
Utilitários	Este módulo é composto de operadores de utilitário usados nos processos do PAM
Utilitários de rede	Fornece vários utilitários e operações para serviços de rede.

Clique na guia Criador, clique em Exibir e selecione Operadores para exibir os nomes de pastas que refletem o mesmo agrupamento de operadores das categorias de operadores que você configura.

Operadores(229)

Filtro

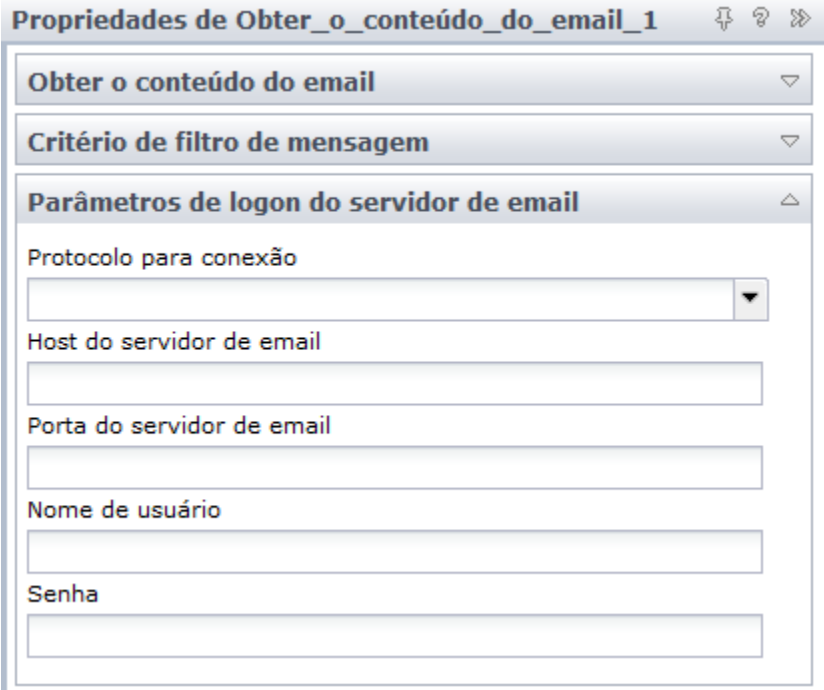
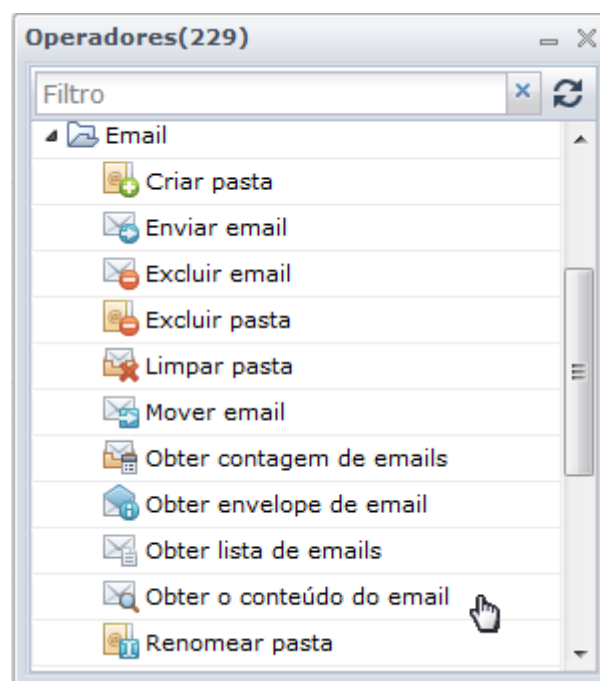
Favotiros
Padrão
Bancos de dados
Catalyst
Controle de processo
Data/hora
Email
Execução de comando
Gerenciamento de arquivos
Gerenciamento de Java
Não categorizado
Serviços de diretório
Serviços web
Transferência de arquivos
Utilitários
Utilitários de rede

Os criadores de conteúdo selecionam operadores na paleta Operadores para criar processos automatizados. Cada operador executa uma operação específica. Para ajudar os criadores a localizar rapidamente o operador adequado, o CA Process Automation agrupa os operadores em categorias que representam o uso comum. Por exemplo, todos os operadores que são usados para transferência de arquivos com o FTP são agrupados em uma pasta chamada Transferência de Arquivos.

Você configura os valores de categoria do operador no nível Domínio. Os valores são herdados no nível de ambiente e, em seguida, no nível de touchpoint do Orquestrador ou agente. É possível substituir os valores herdados em qualquer nível. Os operadores então herdam os valores padrão da categoria do operador. Os criadores de conteúdo podem aceitar ou substituir esses valores.

Mais informações:

Configuração da categoria e herança do operador (na página 304)

Exemplo: configurações de categoria usadas pelo operador

Ao definir as configurações do nível Domínio para cada categoria na guia Módulos, considere os valores que são normalmente usados pelos operadores. Se você definir as configurações com base no caso mais usado, a configuração nos níveis inferiores será feita somente para exceções.

Considere a configuração em Propriedades do email, onde o protocolo padrão para conexão está definido como IMAP e a porta do servidor de email padrão está definida como 143. Configure o servidor de email padrão, o nome de usuário padrão e a senha padrão.

Quando um criador de conteúdo automatiza um processo de email, um dos operadores disponíveis para uso é Obter o conteúdo do email.

Quando um criador de conteúdo arrasta o operador Obter o conteúdo do email para a tela, as Propriedades Get_Email_Content_1 são exibidas. Observe a semelhança entre as propriedades de email configuradas na guia Módulos na guia Configuração e os parâmetros de logon do servidor de email para as propriedades Get_Email_Content_1 exibidas na guia Criador.

O operador Obter o conteúdo do email herda valores para esses Parâmetros de logon do servidor de email	dos valores da configuração do módulo Email para Propriedades de email
Protocolo para conexão	Protocolo padrão para conexão
Host do servidor de e-mail	Host do servidor de email padrão
Porta do servidor de email	Porta do servidor de email padrão
Nome de usuário	Nome de usuário padrão
Senha	Senha padrão

O criador de conteúdo pode configurar valores específicos para o processo e substituir os valores padrão configurados anteriormente. Ou, o criador de conteúdo pode deixar o campo em branco para que os valores padrão sejam herdados. Neste exemplo, o Protocolo para conexão em branco usa o protocolo IMAP e a Porta do servidor de email em branco usa a porta 143.

Propriedades de Obter_o_conteúdo_do_email_1

Obter o conteúdo do email

Critério de filtro de mensagem

Parâmetros de logon do servidor de email

Protocolo para conexão

Host do servidor de email

Porta do servidor de email

Nome de usuário

Senha

Configurando categorias do operador

Os administradores que podem bloquear o domínio conseguem definir ou alterar as configurações padrão das categorias do operador em nível de domínio. Essas configurações são herdadas. É possível editar essas configurações nos níveis de ambiente, orquestrador e agente. Para obter detalhes, consulte Substituir configurações herdadas por uma categoria de operadores (na página 308).

Os valores padrão para todos os campos de categorias do operador podem ser substituídos em nível de operador. Os valores que você digita para qualquer categoria de operador são todos valores padrão. Quando um operador estiver configurado com um campo em branco, ele herdará o valor padrão do campo correspondente da configuração da categoria. Quando você fizer uma seleção de um valor na guia Módulo, nada será ativado ou desativado. Você pode especificar todos os valores padrão, a seu critério. (Quando você configurar essas mesmas opções no nível do operador, a seleção de uma opção desativará as outras.)

Observação: para obter mais detalhes, consulte a *Referência do criador de conteúdo* para verificar a configuração do operador desses mesmos campos.

Para expandir um campo para uma entrada que é maior do que o espaço fornecido, clique com o botão direito do mouse no campo e selecione Expandir. Uma caixa de diálogo com uma caixa de texto é exibida.

Sobre o Catalyst

O Catalyst está configurado com as seguintes configurações:

- Configurações de propriedades do Catalyst.
- Configurações de segurança do Catalyst.

O Unified Service Model (USM) é um esquema de tipos de objetos e propriedades comuns para os quais os dados de todos os conectores são convertidos. O USM esquema permite a análise de dados de todos os gerenciadores de domínio. Você pode analisar os dados em uma interface comum com formatação idêntica em todos os gerenciadores de domínio.

Os operadores do Catalyst permitem usar conectores do Catalyst em processos automatizados. Os operadores do Catalyst suportam as seguintes interfaces:

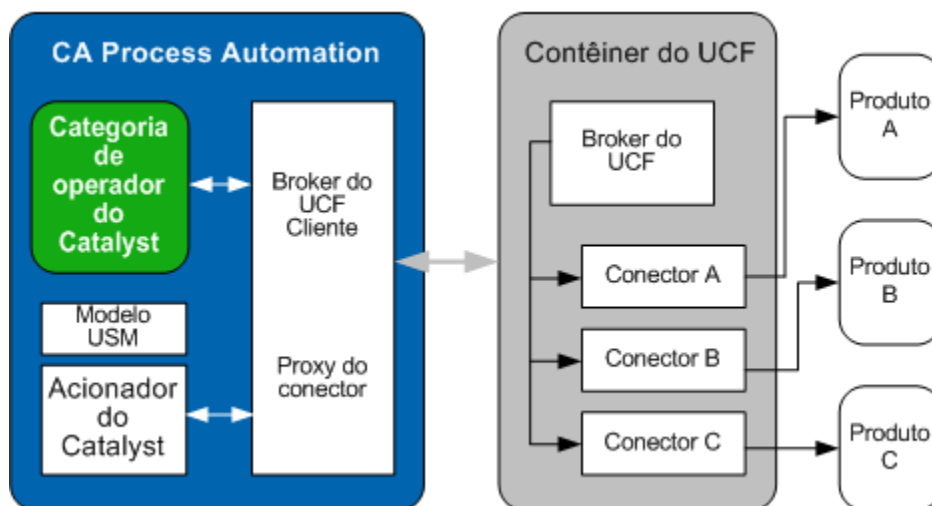
- CRUD (Create, Read, Update, Delete - Criar, Ler, Atualizar, Excluir)
- Execute
- Assinatura de evento

Os operadores exibem os tipos de objetos e propriedades do USM.

O uso do USM comum e das interfaces padrão do UCF fornece compatibilidade do Catalyst com todos os conectores e contêineres do UCF.

O CA Process Automation incorpora os seguintes componentes do UCF-USM:

- Categoria de operador do Catalyst
- Disparador do Catalyst

A categoria do operador do Catalyst e o Disparador do Catalyst são clientes do conector UCF remoto. Eles usam as interfaces do proxy do Broker e do Conector do UCF, como mostra a seguinte ilustração:

Configurar os padrões do Catalyst

Você pode configurar os padrões do Catalyst preenchendo as seguintes guias:

- Propriedades padrão do Catalyst
- Segurança padrão do Catalyst
- Requisições padrão do Catalyst
- Requisições de senha padrão do Catalyst

Observação: os valores de senha são criptografados.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Catalyst e selecione Editar.

   A guia Propriedades padrão do Catalyst é aberta.

3. Configure as propriedades padrão do Catalyst.

   a. Digite o URL padrão apropriado no campo URL do broker do UCF. O operador associado herdará essa configuração. Exemplos de URLs para comunicação segura e básica são os seguintes:

      `http://`*`nome_do_host`*`:7000/ucf/BrokerService`

      `https://`*`nome_do_host`*`:7443/ucf/BrokerService`

   b. Digite o nome apropriado no campo Nome do arquivo de configurações da propriedade do produto. Esse arquivo é usado para personalizar as propriedades exibidas no operador genérico Criar.

4. Clique na guia Segurança padrão do Catalyst e digite a ID de usuário e a senha padrão do Catalyst.

5. Clique na guia Requisições padrão do Catalyst e conclua a configuração.

   a. Clique em Adicionar parâmetro e digite o nome da primeira requisição com seu valor.

   b. Repita essa etapa para cada reivindicação padrão.

   c. Use as setas para cima e para baixo para organizar as reivindicações em sequência, conforme necessário.

6. Clique na guia Requisições de senha padrão do Catalyst e conclua a configuração.

   a. Clique em Adicionar parâmetro e digite o nome da primeira requisição com seu valor.

   b. Repita essa etapa para cada reivindicação de senha padrão.

   c. Use as setas para cima e para baixo para organizar as reivindicações em sequência, conforme necessário.

7. Clique em Salvar e fechar.

8. Clique em Salvar.

9. Selecione Domínio e clique em Desbloquear.

Carregar descritores do Catalyst

Um descritor de conector do Catalyst especifica os recursos do conector, incluindo as operações que ele suporta. Cada operação especifica ainda mais os parâmetros associados. É possível carregar descritores no CA Process Automation. O operador Executar, um operador na categoria de operador do Catalyst, usa os descritores. O produto exibe os descritores carregados em vários níveis:

- Categorias de operação (lista suspensa)
- Operação (lista suspensa)
- Parâmetros (valores do editor)

Você pode carregar um descritor do Catalyst a partir de seu host local para o orquestrador de domínio remoto como um recurso de usuário. O produto replica todos os recursos para cada novo orquestrador.

Siga estas etapas:

1. Clique na guia Configuração.
2. Expanda Gerenciar recursos de usuário no painel esquerdo.
3. Expanda a pasta Repositório, expanda a pasta Recurso do usuário e, em seguida, selecione a pasta ucf. If
4. Clique em Novo.
5. Preencha os campos existentes no painel Adicionar novo recurso, conforme apropriado.

   Observação: deixe o campo Caminho das subpastas de recursos em branco; a Etapa 3 definiu o caminho da subpasta ucf.

6. Clique em Salvar.

   A lista de recursos do usuário exibe o descritor.

Recurso do usuário : ".c2ouserresources/ucf"

Nome	Tipo de arquivo	Caminho do arquivo	Módulo	Descrição
ucfpamconnector-descriptors	jar	.c2ouserresources/ucf/ucfpamconnector-descriptors.jar	itpamucfconnector	ucfpamconnector-descriptors

Observação: o descritor é disponibilizado no operador Executar após você reiniciar o orquestrador. Para obter mais informações sobre o operador Executar na categoria do Catalyst, consulte a *Referência do Criador de Conteúdo*.

Mais informações:

Adicionar um recurso a Recursos do usuário (na página 332)

Sobre a execução de comando

Os operadores Execução de comando permitem executar scripts shell ou programas executáveis em qualquer agente ou orquestrador. Essa categoria oferece acesso a dados e recursos aos dispositivos de rede que suportam os protocolos de interface Telnet e SSH (Secure Shell).

A lista de operadores é a seguinte:

- Executar programa
- Executar script
- Executar comando de SSH
- Executar script SSH
- Executar comando de Telnet
- Executar script de Telnet

Se você estiver executando scripts, siga as convenções do sistema operacional Windows ou UNIX para torná-los executáveis. No CA Process Automation, os scripts retornam o resultado como variáveis de conjuntos de dados do CA Process Automation.

- Nos sistemas UNIX, a primeira linha do script especifica o caminho completo para o intérprete desejado. Por exemplo:

  `#!/bin/sh`

  Especifica a execução usando sh, o shell Bourne em sistemas como o Oracle Solaris. Nos sistemas Linux, essa entrada é um link para outro shell, como o bash. Um operador de script pode executar qualquer script para o qual o host de destino tenha um intérprete.

  Quebre comandos shell como *cp* ou *dir* em um arquivo de script executável.

  `#!/usr/bin/perl`

  Quando colocado no início de um script Perl, informa ao servidor web onde encontrar o executável Perl.

- Para os sistemas Windows, a extensão do nome de arquivo define o intérprete de script. Para o Windows, defina as associações de arquivo para executar o script automaticamente. São aceitas as seguintes extensões:

  `*.ps1`

  Um arquivo PowerShell do Windows.

  `*.exe`

  Um arquivo executável que instala e executa programas e rotinas.

  `*.cmd`

  Um arquivo de lote composto de uma sequência de comandos; semelhante a um arquivo .BAT, mas executado pelo programa CMD.exe e não pelo COMMAND.com.

  `*.vbs`

  Arquivo VBScript.

  `*.wsh`

  Um arquivo de texto Windows Script Host com parâmetros para um script, como um arquivo .vbs; requer o Microsoft WScript ou o Microsoft CScript para abrir o arquivo.

Configurar a execução de comando: propriedades SSH padrão

Ao configurar as propriedades SSH padrão, você deve configurar os seguintes itens:

- As especificações do tipo de terminal.
- Os detalhes de autenticação para efetuar logon em um host remoto.
- (Opcional) Se é necessário alternar os usuários após o logon.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Execução de comando e selecione Editar.
3. Selecione a guia Propriedades SSH padrão.
4. Especifique o tipo de pseudoterminal padrão para solicitar na conexão SSH.

   Observação: VT100 geralmente funciona com hosts do Linux; VT400 geralmente funciona com hosts do Windows.

5. Selecione a porta padrão a ser usada para estabelecer conexão com o host remoto.

   Observação: a porta 22 é a porta TCP/UDP do sistema para o protocolo Secure Shell (SSH).

6. Digite o nome de usuário padrão a ser usado para efetuar logon no host remoto.

7. Especifique os padrões da chave privada:

   a. Indique se uma chave privada será usada para efetuar logon.

      Observação: a alternativa é usar as informações da senha.

   b. Digite a senha padrão a ser usada para efetuar logon no host remoto.

   c. Clique em Procurar (...) e recupere o conteúdo da chave privada (isto é, o conteúdo de uma chave privada padrão para efetuar logon no host remoto).

   d. Digite o caminho para uma chave privada padrão para efetuar logon no host remoto.

   e. Digite a frase secreta para desbloquear o conteúdo da chave privada padrão.

      Observação: a passphrase é obrigatória se a chave privada padrão tiver sido criada com uma passphrase.

8. Especifique os padrões para executar o script ou os comandos especificados como um usuário diferente.

   a. Especifique se é necessário executar o script ou os comandos especificados como um usuário diferente.

   b. Especifique o comando específico do sistema operacional para alternar o usuário no host remoto. O comando su -root alterna usuários para o usuário raiz. Por exemplo:

      ```
      su - <username>
      ```

      ```
      sudo su - <username>
      ```

   c. Digite uma expressão regular para o prompt de texto padrão se o host remoto exigir uma senha para alternar usuários.

      O texto de prompt geralmente é Password: ou password:. A expressão regular .*assword: corresponde a qualquer entrada (incluindo novas linhas) e uma letra P maiúscula ou p minúscula, seguida por assword:œ.

   d. Digite a senha padrão a ser digitada no prompt de texto se o host remoto exigir uma senha para alternar usuários.

   e. Digite uma expressão regular para o prompt de comando que indica que o host remoto está pronto para os comandos como o usuário alternado.

      Prompts de comando típicos são # (hash), > (maior que) e ? (ponto de interrogação). A entrada .*[$>?:#] corresponde a qualquer entrada (incluindo novas linhas) seguida por #, >, ?, $ (cifrão) ou : (dois-pontos). Considere os seguintes exemplos:

      ```
      .*[$]
      ```

      ```
      .*[$>?:#]
      ```

      Observação: para utilizar um cifrão em uma expressão regular, coloque-o entre colchetes. Um cifrão sem colchetes possui um significado especial nas expressões regulares.

9. Clique em Salvar e fechar.
10. Clique em Salvar.
11. Selecione Domínio e clique em Desbloquear.

Configurar a execução de comando: propriedades Telnet padrão

A configuração das propriedades Telnet padrão inclui as seguintes tarefas:

- Configurar a conectividade
- Especificar o esquema de logon e detalhes relacionados
- Especificar se é necessário alternar usuários após o logon no host remoto
- Definir os detalhes de alternância

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Execução de comando e selecione Editar.
3. Na guia Propriedades Telnet padrão, selecione o pseudoterminal padrão a ser solicitado na conexão Telnet.
4. Selecione a porta padrão a ser usada para estabelecer conexão com o host remoto.

   Observação: a porta 23 é a porta TCP/UDP do sistema para Telnet.
5. Para Tempo limite da conexão (s), use o controle giratório para selecionar o intervalo (em segundos) de espera antes de atingir o tempo limite de conexão.
6. Selecione um esquema de logon padrão na lista suspensa.
7. Defina os prompts de logon e valores padrão:
   a. Digite uma expressão regular para o prompt de logon (por exemplo, digite. *ogin.*:).
   b. Digite o nome de usuário a ser usado para efetuar logon no host remoto.
   c. Digite uma expressão regular para o prompt de texto padrão que indica que o host remoto exige uma senha para o logon do usuário (por exemplo, digite .*assword.*:).
   d. Digite a senha padrão a ser usada para efetuar logon no host remoto.
8. Digite uma expressão regular para o prompt de comando que indica que o host remoto está pronto para os comandos (por exemplo, digite .*[$>?:#]).).

   Observação: para utilizar um cifrão em uma expressão regular, coloque-o entre colchetes. Por exemplo, [$].

9. Selecione o intervalo (em segundos) que a conexão aguarda até que o prompt envie os comandos.

10. Defina os valores padrão para alternar usuários:

    a. Especifique se deseja alternar usuários antes de executar o script ou os comandos especificados.

    b. Digite o comando específico do sistema operacional para alternar o usuário no host remoto.

       Observação: o comando su -root alterna o usuário para o usuário raiz.

       Considere os seguintes exemplos:

       ```
       su - <username>
       ```

       ```
       sudo su - <username>
       ```

    c. Digite uma expressão regular para o prompt de texto padrão para alterar a senha do usuário (por exemplo, digite .*assword.*:).

    d. Digite a senha padrão a ser digitada no prompt de texto de senha.

    e. Digite uma expressão regular para o prompt que indica que o host remoto está pronto para os comandos como o usuário alternado.

       Observação: hash (#), maior que (>) e ponto de interrogação (?) são prompts de comando típicos. Digite .*[$>?:#] para corresponder a qualquer entrada (incluindo novas linhas) seguida por #, >, ?, $ (cifrão) ou : (dois-pontos).

       Considere os seguintes exemplos:

       ```
       .*[$]
       ```

       ```
       .*[$>?:#]
       ```

       Observação: para utilizar um cifrão em uma expressão regular, coloque-o entre colchetes. Por exemplo, [$].

11. Clique em Salvar e fechar.

12. Clique em Salvar.

13. Selecione Domínio e clique em Desbloquear.

Configurar a execução de comando: propriedades da execução de comando padrão do Unix

É possível configurar as propriedades de execução padrão para os comandos do UNIX.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.

2. Clique na guia Módulos, clique com o botão direito do mouse em Execução de comando e selecione Editar.

3. Selecione a guia Propriedades da execução de comando padrão do Unix.
4. Digite um dos intérpretes do comando shell a seguir para usar como padrão para comandos shell e de perfil:

   `/bin/bash`

   `/bin/csh`

   `/bin/ksh`
5. Digite o nome do arquivo de script de shell padrão para interpretar antes de iniciar um processo de usuário para o qual nenhum perfil está especificado.

   O perfil pode conter qualquer comando não interativo compreendido pelo intérprete de shell.
6. Especifique as credenciais de usuário padrão.
   a. Selecione um dos valores a seguir para especificar que os operadores de processo usem a opção selecionada quando as credenciais de usuário não forem especificadas:
      - (Padrão) Usa como padrão o usuário no qual o touchpoint é executado.

        Os operadores de processo usam as credenciais de usuário com as quais o processo do agente ou orquestrador está em execução.
      - Usa como padrão o usuário Padrão especificado.

        Os operadores de processo usam as credenciais de usuário configuradas como Usuário padrão e Senha padrão.
      - Sem padrão.

        Os operadores de processo usam as credenciais de usuário fornecidas no tempo de execução.
   b. Considere as seguintes implicações de especificar padrões para a ID de usuário e a senha:
      - Para impedir os usuários de definir e iniciar processos por meio do CA Process Automation aos quais, de outra forma, não teriam acesso, especifique uma ID de usuário somente com as permissões necessárias.
      - Deixe a ID de usuário e a senha em branco para obrigar os usuários a fornecer esses valores quando iniciarem processos por meio do CA Process Automation.
   c. Se apropriado, digite a conta de shell padrão a ser usada ao iniciar processos do usuário que não tenham nome de usuário e senha.
   d. Se apropriado, digite a senha da conta de usuário do Shell.

      Observação: as senhas que fazem parte das configurações de Execução de comando são protegidas e não podem ser modificadas por um programa, referenciadas ou transferidas para métodos externos.
   e. Digite a Senha padrão novamente para confirmá-la.

7. Considere as seguintes implicações de especificar padrões para a ID de usuário e a senha:
   - Para impedir os usuários de definir e iniciar processos por meio do CA Process Automation aos quais, de outra forma, não teriam acesso, especifique uma ID de usuário somente com as permissões necessárias.
   - Deixe a ID de usuário e a senha em branco para obrigar os usuários a fornecer esses valores quando iniciarem processos por meio do CA Process Automation.
8. Se apropriado, digite a conta de shell padrão a ser usada ao iniciar processos do usuário que não tenham nome de usuário e senha.
9. Se apropriado, digite a senha da conta de usuário do Shell.

   Observação: as senhas que fazem parte das configurações de Execução de comando são protegidas e não podem ser modificadas por um programa, referenciadas ou transferidas para métodos externos.
10. Digite a Senha padrão novamente para confirmá-la.
11. Indique se é necessário carregar o perfil de usuário associado ao usuário padrão e à senha padrão especificados.
12. Indique se deseja desativar a verificação de senha.
13. Clique em Salvar e fechar.
14. Clique em Salvar.
15. Selecione Domínio e clique em Desbloquear.

Configurar a execução de comando: Propriedades da execução de comando padrão do Windows

É possível configurar as propriedades de execução padrão para os comandos do Windows.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Execução de comando e selecione Editar.
3. Selecione a guia Propriedades da execução de comando padrão do Windows.
4. Digite o intérprete do comando shell padrão para usar em comandos shell e de perfil. Por exemplo:

   ```
   cmd.exe
   ```

   Observação: não digite Command.exe.

5. Digite o nome do arquivo de script de shell padrão para interpretar antes de iniciar um processo de usuário para o qual nenhum perfil está especificado.

   O intérprete do comando que o programa Shell especifica interpreta o arquivo de perfil. O perfil pode conter qualquer comando não interativo compreendido pelo intérprete de shell.

6. Especifique as credenciais de usuário padrão.

   a. Selecione um dos valores a seguir para especificar que os operadores de processo usem a opção selecionada quando as credenciais de usuário não forem especificadas:

      - (Padrão) Usa como padrão o usuário no qual o touchpoint é executado.

        Os operadores de processo usam as credenciais de usuário com as quais o processo do agente ou orquestrador está em execução.

      - Usa como padrão o usuário Padrão especificado.

        Os operadores de processo usam as credenciais de usuário configuradas como Usuário padrão e Senha padrão.

      - Sem padrão.

        Os operadores de processo usam as credenciais de usuário fornecidas no tempo de execução.

   b. Considere as seguintes implicações de especificar padrões para a ID de usuário e a senha:

      - Para impedir os usuários de definir e iniciar processos por meio do CA Process Automation aos quais, de outra forma, não teriam acesso, especifique uma ID de usuário somente com as permissões necessárias.

      - Deixe a ID de usuário e a senha em branco para obrigar os usuários a fornecer esses valores quando iniciarem processos por meio do CA Process Automation.

   c. Se apropriado, digite a conta de shell padrão a ser usada ao iniciar processos do usuário que não tenham nome de usuário e senha.

   d. Se apropriado, digite a senha da conta de usuário do Shell.

      Observação: as senhas que fazem parte das configurações de Execução de comando são protegidas e não podem ser modificadas por um programa, referenciadas ou transferidas para métodos externos.

   e. Digite a Senha padrão novamente para confirmá-la.

7. Considere as seguintes implicações de especificar padrões para a ID de usuário e a senha:
   - Para impedir os usuários de definir e iniciar processos por meio do CA Process Automation aos quais, de outra forma, não teriam acesso, especifique uma ID de usuário somente com as permissões necessárias.
   - Deixe a ID de usuário e a senha em branco para obrigar os usuários a fornecer esses valores quando iniciarem processos por meio do CA Process Automation.
8. Se apropriado, digite a conta de shell padrão a ser usada ao iniciar processos do usuário que não tenham nome de usuário e senha.
9. Se apropriado, digite a senha da conta de usuário do Shell.

   Observação: as senhas que fazem parte das configurações de Execução de comando são protegidas e não podem ser modificadas por um programa, referenciadas ou transferidas para métodos externos.
10. Digite a Senha padrão novamente para confirmá-la.
11. Indique se é necessário carregar o perfil de usuário associado ao usuário padrão e à senha padrão especificados.
12. Clique em Salvar e fechar.
13. Clique em Salvar.
14. Selecione Domínio e clique em Desbloquear.

Sobre bancos de dados

A categoria Bancos de dados de operadores usam a tecnologia Java Database Connectivity (JDBC). A tecnologia JDBC oferece suporte à conectividade em um ambiente heterogêneo entre a linguagem de programação Java e os bancos de dados, como o Microsoft SQL Server. A categoria Bancos de dados não oferece suporte a operações administrativas, como a interrupção de um servidor de banco de dados. As informações de conexão podem ser fornecidas com o servidor, a porta e o SID (System Identifier - Identificador de Sistema), ou com uma entrada TNSNAMES em tnsnames.ora. O arquivo tnsnames.ora é o arquivo de configuração de nome do serviço Oracle.

A categoria Bancos de dados inclui configurações para os seguintes bancos de dados:

- Oracle
- MSSQL
- MySQL
- Sybase

Para usar a categoria de operadores Bancos de dados com um RDBMS de um fornecedor diferente dos que o CA Process Automation usa, instale o driver apropriado.

Observação: consulte "Instalar drivers JDBC para conectores JDBC" no *Guia de Instalação* para obter detalhes.

Mais informações:

Habilitar a segurança integrada do Windows para o módulo JDBC para MSSQL Server (na página 286)

Configurar bancos de dados: propriedades padrão do Oracle

Você pode configurar a categoria de operadores para bancos de dados Oracle.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Bancos de dados e selecione Editar.

3. Na guia Propriedades padrão do Oracle, selecione um dos seguintes valores como o tipo padrão de driver JDBC do Oracle. Use uma versão de JDBC que corresponda à versão do JDK (Java Development Kit - Kit de Desenvolvimento Java).

   thin

   O tipo de thin driver é para uso do cliente sem instalação do Oracle. O Thin Driver se conecta ao banco de dados Oracle com sockets Java.

   OCI

   O tipo de driver OCI é para uso do cliente com instalação do Oracle. Os drivers OCI usam a OCI (Oracle Call Interface) para interagir com o banco de dados Oracle.

   KPRB

   O tipo de driver KBRP é usado para criar procedimentos e disparadores armazenados no banco de dados Java.

4. Aceite a entrada de driver padrão (oracle.jdbc.OracleDriver) ou altere a entrada de driver.
5. Digite o local do servidor Oracle e as credenciais de logon:
   a. Digite o host do servidor em que o banco de dados Oracle está em execução.
   b. Digite a porta padrão para o banco de dados Oracle.
   c. Digite o nome de usuário padrão para o usuário do banco de dados Oracle.
   d. Digite a senha associada ao nome de usuário especificado.
6. Digite a ID do serviço Oracle.
7. Digite a origem do conteúdo de tnsnames.ora no diretório do Oracle.

   O arquivo Nomes TNS do Oracle converte um alias do banco de dados local em informações que permitem a conectividade com o banco de dados. Essas informações incluem endereço IP, porta e ID do serviço de banco de dados.

8. Aceite o número máximo padrão de linhas a serem recuperadas (10) ou selecione outro valor até 512.

9. Digite o método de criptografia de dados padrão. Considere a possibilidade de digitar um dos valores a seguir, sendo que RCA_128 e RCA_256 destinam-se apenas a edições locais:
   - RC4_40
   - RC4_56
   - RC4_128
   - RC4_256
   - DES40C
   - DES56C
   - 3DES112
   - 3DES168
   - SSL
   - AES128
   - AES256
   - AES192
10. Digite o padrão de somas de verificação que o Oracle suporta. Consulte a documentação do Oracle.
11. Clique em Salvar e fechar.
12. Clique em Salvar.
13. Selecione Domínio e clique em Desbloquear.

Configurar bancos de dados: propriedades padrão do MSSQL Server

Você pode configurar a categoria de operadores Bancos de dados para o MSSQL Server.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Bancos de dados e selecione Editar.
3. Clique na guia Propriedades padrão do MSSQL Server.
4. Aceite com.microsoft.sqlserver.jdbc.SQLServerDriver como o driver padrão para MSSQL Server.
5. Digite o nome do host ou endereço IP do host em que o MSSQL Server está em execução, para usar como padrão.
6. Digite a porta padrão do MSSQL Server (geralmente é 1433).

7. Especifique as credenciais padrão para o usuário do banco de dados do MSSQL.
   - Digite um nome de usuário.
   - Digite a senha associada ao nome de usuário especificado.
8. Aceite o número máximo padrão de linhas a serem recuperadas (10) ou selecione outro valor até 512.
9. Digite o nome padrão do banco de dados do MSSQL.
10. Digite o nome padrão da instância do MSSQL.
11. Clique em Salvar e fechar.
12. Clique em Salvar.
13. Selecione Domínio e clique em Desbloquear.

Habilitar a segurança integrada do Windows para o módulo JDBC para MSSQL Server

Você pode permitir que os operadores da categoria Bancos de dados do Microsoft SQL Server (MSSQL) usem a segurança integrada. Esses operadores podem usar a segurança integrada ao se conectar a touchpoints em hosts em execução em sistemas operacionais Windows.

Um operador Bancos de dados é um operador da categoria Bancos de dados. Hosts de destino são os hosts com um agente ou orquestrador. Para cada host de destino que um operador Bancos de Dados pode acessar, copie sqljdbc_auth.dll no caminho do sistema desse host. Esse processo configura a categoria Bancos de dados para MSSQL para que ela use a segurança integrada com Autenticação do Windows.

Você pode ativar a segurança integrada do Windows para a categoria Bancos de dados do MSSQL Server.

Siga estas etapas:

1. Se você estiver usando a versão do driver do Microsoft SQL Server fornecida com o CA Process Automation, baixe a versão 3.0 do driver no site da Microsoft. Caso contrário, localize (ou baixe novamente) a versão completa do driver.
2. Localize o sqljdbc_auth.dll fornecido ou baixado que corresponde ao hardware onde o agente ou orquestrador está em execução.

3. Copie o sqljdbc_auth.dll para uma pasta do sistema de cada agente ou orquestrador do CA Process Automation que esteja em execução em um ambiente operacional Windows.

   Para determinar o caminho do sistema, execute *uma* das seguintes ações:

   - Insira o seguinte comando em um prompt de comando:

     echo %PATH%

     O caminho do sistema é exibido.

   - Vá para Iniciar, Configurações, Painel de controle, Sistema, Avançado (Configurações avançadas do sistema), Variáveis de ambiente. O caminho do sistema é exibido na variável PATH.

4. Reinicie o agente ou o orquestrador.

Observações:

- Ao criar um URL de conexão sem segurança integrada, especifique o nome do usuário e a senha. Para usar a segurança integrada, não especifique o nome do usuário e a senha.
- Acrescente ;integratedSecurity=true no URL de conexão. Por exemplo:

```
jdbc:sqlserver://localhost ... ;integratedSecurity=true
```

Configurar bancos de dados: propriedades padrão do MySQL

Você pode configurar a categoria de operadores Bancos de dados para o MySQL Server.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Bancos de dados e selecione Editar.
3. Clique na guia Propriedades padrão do MySQL Server.
4. Aceite com.mysql.jdbc.Driver como o driver padrão para MySQL.
5. Identifique o host em que o banco de dados do MySQL está em execução.
6. Digite a porta do banco de dados padrão do MySQL, por exemplo, 3306.
7. Digite as credenciais de logon padrão para o banco de dados padrão do MySQL.
   a. Digite o nome de usuário padrão para o usuário do banco de dados do MySQL.
   b. Digite a senha associada ao nome de usuário especificado.
8. Aceite o número máximo padrão de linhas a serem recuperadas (10) ou selecione outro valor até 512.
9. Digite o nome padrão do banco de dados do MySQL.

10. Clique em Salvar e fechar.
11. Clique em Salvar.
12. Selecione Domínio e clique em Desbloquear.

Configurar bancos de dados: propriedades padrão do Sybase

Você pode configurar a categoria de operadores Bancos de dados para o Sybase.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Bancos de dados e selecione Editar.
3. Clique na guia Propriedades padrão do Sybase.
4. Selecione um dos seguintes valores para o sistema de banco de dados relacional padrão do Sybase:
   - ASA (Adaptive Server Anywhere)
   - ASE (Adaptive Server Enterprise)
5. Aceite Tds ou digite outro protocolo de conexão padrão.
6. Aceite com.sybase.jdbc2.jdbc.SybDriver ou digite outro driver padrão.
7. Especifique o local do banco de dados do Sybase.
   a. Identifique o host do servidor.
   b. Digite a porta padrão.
8. Digite as credenciais de logon padrão para o banco de dados padrão do Sybase.
   a. Digite o nome de usuário padrão.
   b. Digite a senha associada ao nome de usuário especificado.

9. Aceite 10 como o número máximo padrão de linhas a serem recuperadas ou selecione outro valor até 512.
10. Especifique a quantidade de memória usada pelo driver para armazenar em cache os dados do conjunto de resultados sem diferenciação de maiúscula e minúscula de uma das seguintes maneiras:

    -1

    Todos os dados são armazenados em cache.

    0

    Até 2 GB de dados estão armazenados em cache.

    s

    Especifica o tamanho do buffer, em KB, em que o valor é um múltiplo de 2 (um número par). Quando o limite especificado é atingido, os dados são armazenados em cache.
11. Indique se é necessário usar o mecanismo compatível com o JDBC v3.0 como a solução alternativa padrão de desempenho do lote.

    Observação: se este item não for selecionado, será usado o mecanismo nativo do lote.
12. Clique em Salvar e fechar.
13. Clique em Salvar.
14. Selecione Domínio e clique em Desbloquear.

Sobre o Date-Time

Os operadores na categoria Data e hora podem funcionar em orquestradores. A categoria Data e hora oferece suporte às opções de data e hora para os operadores em outras categorias e operadores condicionais para executar ramificações em um processo. Os exemplos estão a seguir:

- Comparar data e hora atual com uma data e hora especificada.
- Testar se a data atual ocorre em uma regra de calendário.
- Aguardar uma data e hora especificada.

A categoria de operadores Data/hora não tem propriedades configuráveis.

Sobre os Serviços de diretório

A categoria de operadores Serviços de diretório fornece uma interface que oferece suporte ao protocolo LDAP (Lightweight Directory Access Protocol). Os operadores Serviços de diretório podem ser executados em um orquestrador ou agente.

Configurar padrões de serviços de diretório

Você pode configurar Serviços de diretório. A categoria de operadores Serviços de diretório fornece uma interface para suporte a LDAP/AD.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Serviços de diretório e selecione Editar.
3. Especifique um tamanho de lote padrão para retornar resultados da operação, a fim de ajudar o servidor a otimizar o desempenho e a utilização de recursos. Selecione um valor entre 1 e 1000, ou digite 0 para permitir que o servidor determine o tamanho do lote.
4. Selecione um valor para o número máximo de objetos a retornar ao executar o operador Obter o objeto ou Obter usuário.
5. Especifique os seguintes nomes de classe de fábrica:
   a. Aceite o padrão, com.sun.jndi.ldap.LdapCtxFactory, como o nome de classe totalmente qualificado da classe de fábrica que cria um contexto inicial.
   b. Digite uma lista, separada por dois-pontos, de nomes de classe de fábrica de estados totalmente qualificados que podem obter o estado de um objeto especificado. Deixe esse campo em branco para usar o estado padrão de fábrica de classes.
   c. Digite uma lista, separada por dois-pontos, de nomes de classe totalmente qualificados de classes de fábrica que criam um objeto com informações sobre o objeto. Deixe esse campo em branco para usar o padrão de fábrica de classes de objeto.
6. Digite uma lista, separada por dois-pontos, de tags de idiomas, em que as tags são definidas no RFC 1766. Deixe em branco para permitir que o servidor LDAP determine a preferência de idioma.
7. Selecione um dos valores a seguir para especificar como o servidor LDAP lida com as orientações.

   Ignorar

   Ignora as orientações.

   Seguir

   Segue as orientações.

   Acionar

   Retorna a primeira orientação que o servidor encontrar e interrompe a pesquisa.

8. Especifique o mecanismo de autenticação do servidor LDAP para o uso com uma das seguintes entradas:

   Nenhuma

      Não usa autenticação (anônimo).

   Simples

      Usa autenticação fraca (senha com texto não criptografado). Selecione esta opção quando definir o protocolo de segurança como SSL.

   Lista separada de mecanismo SASL separada por espaço.

      Permite que o LDAP ofereça suporte a qualquer tipo de autenticação aceita pelo servidor e o cliente do LDAP.

9. Indique o protocolo de segurança de uma das seguintes maneiras:

   - Digite **ssl** para especificar o protocolo que permite conexões do servidor LDAP por meio de um socket seguro.

     Importante: Ao conectar-se com o Active Directory (AD), digite **ssl** em *minúsculas*. O AD rejeita o valor SSL.

   - Deixe em branco para usar a conectividade básica.

10. Selecione um valor para indicar o valor de tempo limite da conexão em segundos ou digite 0 (zero) para não haver tempo limite.

11. Digite o local do servidor LDAP padrão e as credenciais de logon padrão.

    a. Digite o nome do host ou endereço IP.

    b. Digite a porta padrão para o servidor LDAP. Considere as seguintes portas:

       - 389 - A porta LDAP para LDAP (Lightweight Directory Access Protocol).
       - 636 - A porta LDAP para o protocolo LDAP por TLS/SSL.

    c. Digite a ID do usuário LDAP padrão. Os operadores podem usar esse padrão ou substituí-lo.

    d. Digite a senha padrão do usuário LDAP. Os operadores podem usar esse padrão ou substituí-lo.

12. Digite o DN (Distinguished Name - Nome Diferenciado) base padrão. Os operadores podem usar esse padrão ou substituí-lo.

13. Digite um **uid** ou **cn** como o prefixo de usuário padrão.

14. Clique em Salvar e fechar.

15. Clique em Salvar.

16. Selecione Domínio e clique em Desbloquear.

Sobre Email

A categoria de operadores Email permite que você trabalhe com mensagens e pastas em um servidor de email. Os operadores de email comunicam-se com o servidor de email remotamente, usando um dos seguintes protocolos:

- POP3 (Post Office Protocol versão 3)
- POP3-SSL
- IMAP (Internet Message Application Protocol)
- IMAP-SSL

Alguns operadores, como aqueles que atuam nas pastas, são suportados apenas quando se usa o protocolo IMAP.

Observação: consulte a *Referência do Criador de Conteúdo* para obter detalhes sobre o protocolo suportado por cada operador Email.

Configurar propriedades de email padrão

Você pode definir configurações padrão para os operadores Email.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Email e selecione Editar.
3. Digite o nome do host do servidor SMTP para alertas de email do Java.
4. Digite o endereço de email que será exibido no campo do remetente de alertas de email de saída do Java. Configure totalmente esta conta. Por exemplo:

   `*nome_do_usuário*@*nome_da_empresa*.com`

5. Digite o protocolo padrão usado para receber emails de um servidor remoto ou servidor web remoto.
   - IMAP
   - POP3
   - IMAP-SSL
   - POP3-SSL
6. Identifique o servidor de email padrão do qual o email foi recuperado.

7. Digite a porta padrão do servidor de email padrão para emails de entrada. Considere as seguintes portas:

   143

   A Porta IMAP para uma conexão não segura.

   110

   A Porta POP3 para uma conexão não segura.

   993

   A porta IMAP-SSL para uma conexão segura.

   995

   A porta POP3-SSL para uma conexão segura.

8. Especifique as credenciais padrão para o usuário de email como segue ou deixe em branco se esse valor sempre for especificado em nível de operador.
   a. Digite um nome de usuário.
   b. Digite a senha associada.
9. Clique em Salvar e fechar.
10. Clique em Salvar.
11. Selecione Domínio e clique em Desbloquear.

Sobre o gerenciamento de arquivos

A categoria de operadores Gerenciamento de arquivos pode ser executada em um agente ou orquestrador. Os operadores Gerenciamento de arquivos monitoram a existência ou o status de um arquivo ou diretório. Além disso, os operadores Gerenciamento de arquivos procuram padrões específicos dentro do conteúdo de um arquivo. As regras de interface portável entre sistemas operacionais controlam os padrões na correspondência de padrões de texto. Essa função pode ser usada para determinar um processamento adicional em um Processo. Por exemplo, os operadores Gerenciamento de arquivos podem aguardar um arquivo XML contendo padrões que exigem processamento. O Gerenciamento de arquivos pode procurar mensagens de erro no conteúdo dos arquivos de log.

A categoria de operadores Gerenciamento de arquivos observa os arquivos ou monitora o conteúdo de um arquivo no destino. Os arquivos podem estar em outro computador ou unidade de rede, porém, precisam ser visíveis aos operadores. Todos os operadores Gerenciamento de arquivos (como criação de caminhos de diretório ou verificação do conteúdo do arquivo) são executados como Administrador ou como o usuário que iniciou o touchpoint.

Condições específicas para teste ou espera incluem:

- A aparência de um arquivo.
- A ausência de um arquivo.
- Condições sobre o tamanho de um arquivo.
- A data/hora da última modificação.
- A existência de uma sequência de caracteres ou um padrão em um arquivo (com base em máscaras de interface portável entre sistemas operacionais)

Configurar o gerenciamento de arquivos

Você pode definir configurações padrão para operadores na categoria Gerenciamento de arquivos. A menos que seja mencionado, os campos de referência se aplicam aos sistemas operacionais UNIX ou Linux e Microsoft Windows.

Observação: para expandir um campo para uma entrada da janela Gerenciamento de arquivos que excede o espaço fornecido, clique com o botão direito do mouse no campo e selecione Expandir.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Gerenciamento de arquivos e selecione Editar.

3. Execute as seguintes etapas na janela Gerenciamento de Arquivos:

   a. Clique em Propriedades de gerenciamento de arquivos padrão do Windows ou Propriedades de gerenciamento de arquivos padrão do Unix, conforme apropriado para o sistema operacional que você estiver configurando.

   b. Preencha os campos a seguir, se você definir o campo Requer credenciais de usuário como Padrões para o usuário especificado abaixo:

      - Usuário
      - Senha
      - Confirmar senha

   c. (UNIX) Defina o shell do sistema do operador. Por exemplo, digite um dos seguintes valores para Shell:

      - /bin/bash
      - /bin/csh/
      - /bin/ksh

   d. (UNIX) Marque ou desmarque a caixa de seleção Desativar verificação de senha, dependendo se o produto deverá verificar a senha de usuário quando alternar usuários.

   e. Digite o comando que compacta um arquivo ou diretório no campo Utilitário de compactação. Por exemplo:

      ```
      WZZIP -P -r {0} {1}
      ```

      ```
      gzip -qrf {0}
      ```

      - {0} é o nome do arquivo compactado de saída.
      - {1} define o nome do arquivo de origem para compactar.

   f. Digite o comando que extrai um arquivo ou diretório compactado no campo Descompactar utilitário. Por exemplo:

      ```
      WZUNZIP -d -o -yO {0}
      ```

      ```
      gunzip -qrf {0}
      ```

      {0} define o nome do arquivo compactado a ser extraído.

4. Clique em Salvar e fechar.

5. Clique em Salvar.

6. Selecione Domínio e clique em Desbloquear.

Sobre a transferência de arquivos

A categoria Transferência de arquivo funciona como um cliente de FTP (File Transfer Protocol) que oferece suporte a operadores de arquivo remotos em um processo. Os operadores da categoria Transferência de arquivos podem ser executados em um orquestrador ou em touchpoints do agente. A categoria Transferência de arquivo oferece suporte a todos os comandos suportados pelo FTP padrão, incluindo:

- Transferências de arquivos de/para um host remoto com suporte a FTP.
- Obtenção de informações do arquivo/diretório de um host remoto.
- Exclusão de um arquivo ou diretório.
- Renomeação de um arquivo/diretório.

Não há pré-requisitos para operadores com base em FTP, usando FTP padrão e servidores FTP padrão. Para as transferências via SFTP, use o SSH2 e pré-defina o touchpoint para se comunicar com o computador servidor de SFTP com base nas credenciais de nome de usuário e senha.

Estabeleça uma conexão SSH e configure os certificados com um cliente de SSH, antes de usar o SFTP. A CA Technologies fornece um cliente de SSH de teste para o Windows, para que você possa estabelecer a conexão inicial. A maioria dos computadores UNIX já o possui. A vantagem do SFTP é que ele é seguro. Com o SFTP, os dados passam por um túnel criptografado e senhas são autenticadas.

Configurar Transferência de arquivos

Você pode definir configurações padrão para todos os operadores na categoria Transferência de arquivos. Em todos os casos, os valores configurados podem ser substituídos no nível de operador. Para obter mais informações, consulte o tópico Configuração da categoria e herança do operador (na página 304).

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Transferência de arquivos e selecione Editar.
3. Na janela Transferência de arquivos, preencha o campo Porta UDP padrão para Trivial FTP (porta 69 é o valor típico).
4. Clique em Salvar e fechar.
5. Clique em Salvar.
6. Selecione Domínio e clique em Desbloquear.

Mais informações:

Substituir configurações herdadas por uma categoria de operadores (na página 308)

Sobre o Gerenciamento de Java

Os operadores Gerenciamento de Java podem ser executados em um agente ou um orquestrador. Esses operadores executam várias tarefas nos recursos Java ManagedBeans (MBeans) usando a tecnologia Java Management Extensions (JMX). Os operadores usam um nome de usuário e senha especificados para se conectarem a um URL de serviço JMX ou um servidor JMX em um host e uma porta especificados.

Operadores específicos executam as seguintes tarefas:

- Recuperar atributos MBeans.
- Chamar métodos MBeans usando parâmetros especificados.
- Definir valores dos atributos MBeans.

A categoria de Gerenciamento de Java não tem propriedades configuráveis.

Sobre Utilitários de rede

Os operadores da categoria Utilitários de rede podem ser executados em orquestradores e agentes e interagir com dispositivos ou gerenciadores SNMP (como gerenciadores de rede). Os operadores de Utilitários de rede determinam o estado de um elemento de configuração de um dispositivo IP.

Os operadores Utilitários de rede geram alertas com base no SNMP (interceptações) para dispositivos ou gerenciadores de rede. A categoria Utilitários de rede foi projetada para influenciar um processo, e não para implementar um monitor de rede completo.

Os usuários podem chamar os operadores a partir de Utilitários de rede para:

- Obtenha o valor das variáveis remotas do MIB (Management Information Base) e use seus valores no Processo (por exemplo, como parâmetros ou condições).
- Aguarde condições no valor das variáveis remotas do MIB.
- Configure as variáveis remotas do MIB para afetar o comportamento de dispositivos externos.
- Envie SNMP interceptações para relatar erros e condições especiais para plataformas de gerenciamento SNMP (por exemplo, Tivoli, HP OpenView ou ISM).

Os operadores Utilitários de rede estão disponíveis em hosts com sistemas operacionais UNIX e Windows. O módulo Utilitários de rede identifica as variáveis remotas do MIB por suas IDs de objeto (OIDs).

Configurar Utilitários de rede

Você pode configurar a categoria de operadores Utilitários de rede.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Transferência de arquivos e selecione Editar.
3. Clique com o botão direito do mouse em Utilitários de rede e selecione Editar.
4. No campo Frequência de sondagem (s), especifique a frequência com que um operador Utilitários de rede obtém, de maneira sincronizada, o identificador de objeto do dispositivo (OID do SNMP) para uma variável de SNMP.
5. Clique em Salvar e fechar.
6. Clique em Salvar.

   O processo de configuração aplica as alterações feitas na configuração do produto no nível de módulo.
7. Selecione Domínio e clique em Desbloquear.

Sobre o Controle de processo

Os operadores da categoria Controle de processo podem ser executados apenas em touchpoints do orquestrador. Os operadores Controle de processo têm as seguintes funções:

- Iniciam e interpretam os processos do CA Process Automation
- Chamam outras categorias para executar os operadores em uma instância de objeto do processo
- Aplicam dependências
- Monitoram as chamadas de categoria e baseiam como ramificações subsequentes do processo são executadas nos resultados de invocação

Quando um processo é iniciado, o produto cria uma cópia (instância) do processo. As alterações feitas na cópia não afetam outras cópias ou o processo original. Você pode iniciar um processo de uma das seguintes maneiras:

- Com o Criador de formulário.
- A partir de uma programação.
- A partir de outro processo.
- A partir de um aplicativo externo que usa um disparador do CA Process Automation.
- A partir de um aplicativo externo que usa chamadas SOAP. Consulte a *Referência da API de serviços web*.

Se você estiver usando arquiteturas altamente descentralizadas, pense em definir grupos lógicos de categorias de operadores em um ambiente e configurar Controle de processo em um touchpoint selecionado em cada grupo. Nessa configuração, o produto inicia processos no touchpoint que executa os operadores Controle de processo para um grupo. Você configura um touchpoint especificamente para executar processos de vários grupos. A execução de processos em uma arquitetura descentralizada oferece os seguintes benefícios:

- Reduz a carga dos computadores individuais
- Reduz o impacto de possíveis incidentes
- Reduz a quantidade de dados trocados em hosts remotos

Configurar o Controle de processo

Você pode definir a configuração padrão para os operadores na categoria Controle de processo.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Controle de processo e selecione Editar.
3. Na janela Controle de processo, preencha o campo Tempo para manter as interações do usuário concluídas (min).
4. Clique em Salvar e fechar.
5. Clique em Salvar.
6. Selecione Domínio e clique em Desbloquear.

Sobre Utilitários

A categoria Utilitários na guia Módulos contém campos que pertencem ao operador Chamar o Java.

Importante: o operador Chamar o Java é executado apenas em um agente e não pode ser configurado para um orquestrador.

A categoria Utilitários permite especificar:

- Caminhos para os jars externos a serem carregados, por padrão, para todos os operadores Chamar o Java.
- O log padrão.

Cada jar que é especificado se torna disponível para o código Java que os operadores Chamar o Java executam. As classes definidas no jars no nível de operador substituem as mesmas classes especificadas no jars para a categoria Utilitários.

Se configurado, os criadores poderão usar o agente de log no contexto do código. Por exemplo:

```
logger.debug()
logger.info()
```

Você pode optar por configurar um log, onde os dados registrados não incluam informações.

Configurar Utilitários

Você poderá definir configurações padrão para o operador Chamar o Java na categoria Utilitários somente se o operador for executado em um agente. Caso contrário, essa categoria do operador não exige configuração. O operador Chamar o Java não têm permissão para ser executado em orquestradores.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Utilitários e selecione Editar.

   A guia Default Invoke Java Operator Properties é exibida.
3. Marque a caixa de seleção Usar o modo Java estrito para impor declarações de variável digitadas, argumentos de método e tipos de retorno no código em tempo de execução do método principal.
4. Clique em Adicionar parâmetro e defina os arquivos JAR externos, conforme apropriado.

5. Para remover um arquivo JAR, selecione um item na lista Jars externo e, em seguida, clique em Excluir.
6. Preencha os campos restantes na janela Utilitários, conforme apropriado.
7. Clique em Salvar e fechar.
8. Clique em Salvar.
9. Selecione Domínio e clique em Desbloquear.

Sobre os serviços web

Os operadores Serviços web são executados em orquestradores e agentes. Dois dos operadores fornecem uma interface para os serviços remotos expostos pelo SOAP. Esses operadores:

- Cria uma solicitação SOAP.

  Os dados podem ser extraídos em tempo de execução dos conjuntos de dados e variáveis existentes do CA Process Automation ou de fontes externas.
- Envia a solicitação SOAP para a categoria de operadores Serviços web apropriada que foi especificada no projeto ou no tempo de execução.
- Recupera a resposta para manipulação de condições de erro conforme apropriado.
- Analisa a resposta de entrada e armazena os resultados nos Conjuntos de dados do CA Process Automation acessados pelos Operadores subsequentes em um Processo.
- Uma chamada assíncrona envia a solicitação e, depois de receber uma confirmação, aguarda uma resposta do destino remoto. As chamadas assíncronas usam uma abordagem mais complexa de envio e recebimento do que as chamadas síncronas. Os Operadores subsequentes em um Processo acessam os dados retornados.

O módulo Serviços web também permite automatizar instalações de gerenciamento de dados em uma rede usando HTTP. Por exemplo, os criadores de conteúdo podem desenvolver processos que automatizam serviços RESTful por meio de operadores HTTP. Quando um operador HTTP estiver configurado com um campo em branco, ele herdará o valor padrão do campo correspondente da configuração da categoria pai. Portanto, quando você fizer uma seleção para um campo da categoria de operadores, nada será ativado ou desativado. Você pode especificar todos os valores padrão, a seu critério. Quando você configurar essas mesmas opções no nível do operador, a seleção de uma opção desativará as outras.

Configurar Serviços web

Você pode definir configurações padrão para operadores na categoria Serviços web.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em Serviços web e selecione Editar.
3. Na janela Serviços web, clique em Propriedades dos serviços web padrão e, em seguida, revise ou atualize os campos, conforme apropriado.
4. Clique em Propriedades HTTP dos serviços web padrão e, em seguida, revise ou atualize os campos, conforme apropriado.
5. Clique em Salvar e fechar.
6. Clique em Salvar.
7. Selecione Domínio e clique em Desbloquear.

Configurar valores para um grupo de operadores personalizados

Você pode configurar valores para as variáveis definidas para um grupo de operadores personalizados selecionado. Os grupos de operadores personalizados são definidos na guia Configuração do grupo de um editor de operador personalizado.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Módulos, clique com o botão direito do mouse em um grupo do operador personalizado e selecione Editar.

   O grupo de operadores personalizados selecionado é exibido. O produto exibe inicialmente as páginas e as variáveis sem valores.
3. Em cada campo ou matriz exibida, insira o valor a ser usado como padrão.

   Os valores padrão podem ser substituídos no nível de ambiente e no nível do operador.
4. Clique em Salvar e fechar.

5. Clique em Salvar.
6. Quando terminar de configurar as categorias de operador e os grupos de operadores personalizados na guia Módulos, selecione Domínio e clique em Desbloquear.

Observação: quando você exclui uma variável ou altera o tipo de dados da variável, o produto não publica as alterações para o domínio ou os ambientes associados.

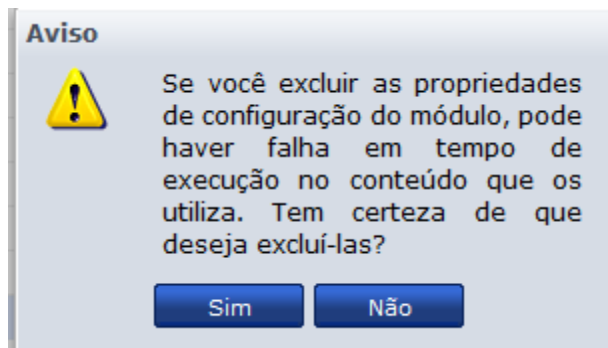
Excluir uma configuração de grupo de operadores personalizados

Os administradores podem usar a guia Módulos no Navegador de Configuração para excluir o grupo de operadores personalizados do domínio e de seus ambientes.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito e selecione Bloquear.
3. Clique com o botão direito do mouse no grupo de operadores personalizados e selecione Excluir.

   O seguinte aviso é exibido:

   Aviso
   Se você excluir as propriedades de configuração do módulo, pode haver falha em tempo de execução no conteúdo que os utiliza. Tem certeza de que deseja excluí-las?
   Sim Não

4. Clique em Sim para confirmar a exclusão.

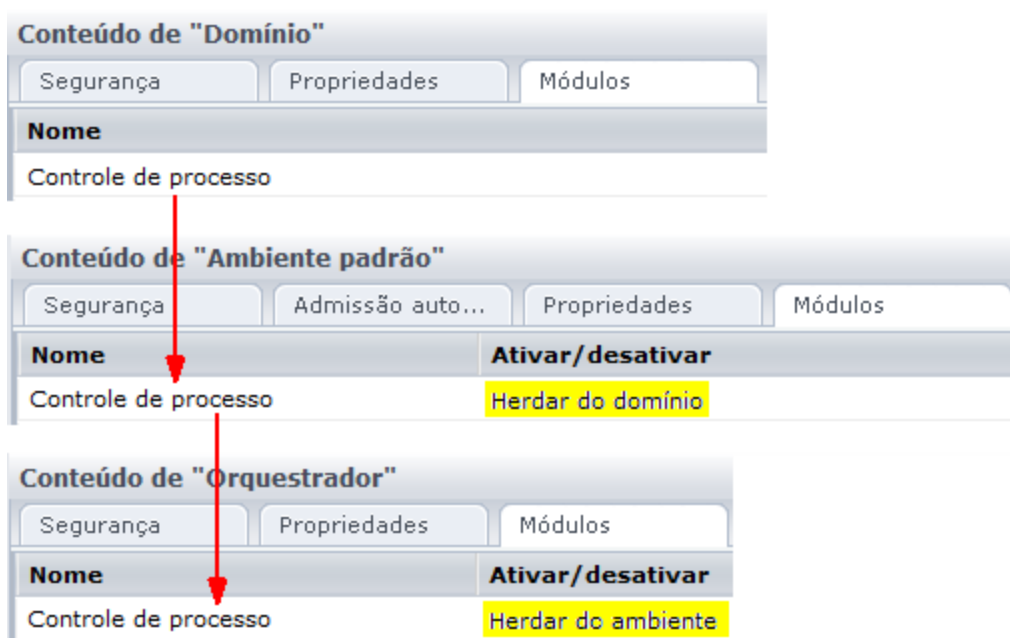
   O CA Process Automation exclui do domínio o módulo de configuração do grupo de operadores personalizados. Se um processo estiver usando o módulo de configuração do grupo de operadores personalizados, a execução do processo falhará.

5. Clique em Salvar.

   A configuração do grupo de operadores personalizados é excluída do domínio e de seu ambiente.

Configuração da categoria e herança do operador

As categorias do operador, como Email ou Transferência de Arquivos, têm definições configuráveis com padrões predefinidos. Os administradores podem editar uma categoria na guia Módulos em vários níveis da hierarquia Domínio. Durante a instalação, as configurações padrão para cada categoria do operador começam no nível Domínio. Essas configurações são marcados como Herdar do domínio no nível do ambiente. No nível Orquestrador, essas configurações são marcados como Herdar do ambiente.

Como mostrado na ilustração a seguir, as configurações da categoria do operador são herdadas do domínio para cada ambiente e de cada ambiente para os orquestradores nesse ambiente. É possível substituir as configurações nos níveis Domínio, Ambiente e Orquestrador.

Os operadores que têm como destino um orquestrador herdam as configurações de categoria de operador desse orquestrador. Os criadores de conteúdo substituem essas configurações herdadas no nível do operador, conforme a necessidade.

Os agentes herdam configurações definidas no nível Domínio, mas os operadores não usam essas configurações. Quando um touchpoint é associado a um agente, a associação inclui um ambiente. No tempo de execução, os operadores que têm um touchpoint como destino usam as propriedades configuradas para o ambiente associado ao touchpoint.

Observação: para os grupos de operadores personalizados definidos pelo usuário, as configurações são herdadas do nível de domínio para o nível de ambiente. Os administradores podem substituir as configurações no nível do ambiente que foram definidas no nível do domínio. Essas configurações não estão disponíveis para substituição nos níveis do orquestrador ou agente.

Mais informações:

Categorias do operador e pastas do operador (na página 266)

Ativar ou desativar uma categoria do operador

As configurações da categoria do operador normalmente são definidas no nível Domínio. Por padrão, as configurações da categoria do operador para ambientes são Herdar do domínio. Por padrão, as configurações da categoria do operador para orquestradores e agentes são definidas como Herdar do ambiente.

Acesse a guia Módulos de um ambiente, orquestrador, ou agente para:

- Ativar uma ou mais categorias do operador.
- Desativar uma ou mais categorias do operador.
- Configurar uma ou mais categorias ativadas.

Siga estas etapas:

1. Clique na guia Configuração.

   O Navegador de configuração é exibido.

2. Execute uma das seguintes ações para estabelecer um bloqueio no nível desejado:
   - Expanda o nó Domínio, selecione o ambiente de destino e clique em Bloquear.
   - Expanda o nó Orquestradores, selecione o orquestrador de destino e clique em Bloquear.
   - Expanda o nó Agentes, selecione o agente de destino e clique em Bloquear.
3. Clique na guia Módulos.
4. Selecione uma categoria do operador, clique na coluna Ativar/desativar e selecione Ativado ou Desativado.
5. Clique em Salvar.
6. Clique em Desbloquear.

Ativar ou desativar um grupo de operadores personalizados

As configurações do grupo de operadores personalizados normalmente são definidas no nível de domínio. Por padrão, as configurações do grupo de operadores personalizados para ambientes são herdadas do domínio.

Acesse a guia Módulos de um ambiente para:

- Ativar um ou mais grupos de operadores personalizados.
- Desativar um ou mais grupos de operadores personalizados.
- Substituir as configurações de um ou mais grupos ativados.

Siga estas etapas:

1. Clique na guia Configuração.

   O Navegador de configuração é exibido.

2. Expanda o nó Domínio, selecione o ambiente de destino e clique em Bloquear.
3. Clique na guia Módulos.
4. Selecione um grupo de operadores personalizados, clique na coluna Ativar/desativar e selecione Ativado ou Desativado.
5. Clique em Salvar.
6. Clique em Desbloquear.

Substituir configurações herdadas por uma categoria de operadores

Um administrador com direitos de administrador de domínio configura categorias para operadores no nível Domínio. Um administrador com direitos de administrador de configuração do ambiente pode substituir as configurações herdadas em qualquer um dos seguintes níveis:

- Ambiente
- orquestrador
- Agente

As configurações da categoria do operador que foram definidas no nível Domínio são exibidas como Herdar do domínio. Essa configuração está em uma lista suspensa, em que outras opções válidas são Ativado e Desativado. Selecione Ativado para editar as configurações herdadas. Selecione Desativado para desativar operadores na categoria selecionada.

Você pode substituir as configurações herdadas em qualquer categoria de operadores em um ou mais níveis.

Siga estas etapas:

1. Clique na guia Configuração.
2. (Opcional) Substitua as configurações selecionadas no nível do ambiente da seguinte maneira:
   a. Clique com o botão direito do mouse no ambiente selecionado e selecione Bloquear.
   b. Clique na guia Módulos.
   c. Selecione uma categoria, clique na lista suspensa para Ativar/desativar e selecione Ativado.
   d. Clique com o botão direito do mouse na categoria e selecione Editar.

      As propriedades da categoria selecionada são exibidas em uma lista rolável.
   e. Altere uma ou mais configurações herdadas.
   f. Clique em Salvar.
   g. Clique com o botão direito do mouse no ambiente e selecione Desbloquear.

3. (Opcional) Substitua as configurações selecionadas no nível do Orquestrador como segue:
    a. Expanda Orquestradores, selecione um orquestrador e clique em Bloquear.
    b. Clique na guia Módulos.
    c. Selecione uma categoria, clique na lista suspensa para Ativar/desativar e selecione Ativado.
    d. Clique com o botão direito do mouse na categoria e selecione Editar.

       As propriedades da categoria selecionada são exibidas em uma lista rolável.
    e. Altere uma ou mais configurações herdadas.
    f. Clique em Salvar.
    g. Clique em Desbloquear.
4. (Opcional) Substitua as configurações selecionadas no nível do agente da seguinte maneira:
    a. Expanda o nó Agentes, selecione um agente e clique em Bloquear.
    b. Clique na guia Módulos.
    c. Selecione uma categoria, clique na lista suspensa para Ativar/desativar e selecione Ativado.
    d. Clique com o botão direito do mouse na categoria e selecione Editar.

       As propriedades da categoria selecionada são exibidas em uma lista rolável.
    e. Altere uma ou mais configurações herdadas.
    f. Clique em Salvar.
    g. Clique em Desbloquear.

Substituir valores herdados para um grupo de operadores personalizados

Um administrador com direitos de administrador de domínio pode configurar grupos de operadores personalizados no nível de domínio. Um administrador com direitos de administrador de configuração do ambiente pode substituir as configurações herdadas no nível do ambiente.

Observação: diferentemente das categorias de operador, não é possível substituir valores de grupos de operadores personalizados no nível do orquestrador ou do agente.

As configurações do grupo de operadores personalizados que foram definidas no nível do domínio são exibidas como herdadas do domínio. Essa configuração está em uma lista suspensa, em que outras opções válidas são Ativado e Desativado. Selecione Ativado para editar as configurações herdadas. Selecione Desativado para desativar os operadores no grupo selecionado.

É possível substituir as configurações que o ambiente selecionado herda do domínio.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique com o botão direito do mouse no ambiente selecionado e selecione Bloquear.
3. Clique na guia Módulos.
4. Selecione uma categoria, clique na lista suspensa para ativar/desativar e selecione Ativado.
5. Clique com o botão direito do mouse na categoria e selecione Editar.

   As propriedades da categoria selecionada são exibidas em uma lista rolável.
6. Altere uma ou mais configurações herdadas.
7. Clique em Salvar.
8. Clique com o botão direito do mouse no ambiente e selecione Desbloquear.

Categorias de operadores e onde os operadores são executados

Alguns operadores são executados apenas em orquestradores, não em touchpoints associados a agentes. Outros operadores são executados em orquestradores e touchpoints do agente, mas não em hosts remotos definidos como destino por touchpoints do proxy ou grupos de hosts. Vários operadores podem ser executados em qualquer tipo de destino. Alguns operadores dentro de uma categoria do operador podem ser executados em orquestradores, mas não em touchpoints do agente. Outros operadores dentro da mesma categoria podem ser executados em orquestradores e touchpoints do agente. A capacidade de execução em um determinado tipo de destino não é perfeitamente mapeado para a categoria do operador.

Observação: consulte Onde os operadores podem ser executados no *Guia de Referência do Criador de Conteúdo* para obter informações sobre os destinos válidos para cada operador.

Capítulo 13: Administrar disparadores

Aplicativos que não podem fazer chamadas SOAP podem usar os disparadores como alternativa. O uso de chamadas SOAP é recomendado em vez dos disparadores, porque elas são mais eficientes.

Os disparadores permitem que aplicativos externos iniciem um processo no CA Process Automation. Um disparador chama o processo do CA Process Automation que está definido no conteúdo XML ou em uma SNMP trap. O conteúdo XML pode ser entregue para o local do arquivo ou o endereço de email configurado. O conteúdo da SNMP trap é enviado em um OID correspondente a uma expressão regular configurada. O CA Process Automation escuta as SNMP traps de entrada na respectiva porta configurada (162 por padrão).

Esta seção contém os seguintes tópicos:

Como configurar e usar disparadores

Para aplicativos externos que não podem emitir chamadas SOAP para iniciar processos do CA Process Automation, o CA Process Automation fornece quatro disparadores pré-definidos. Você pode configurar os disparadores para ativar a inicialização de processos a partir de qualquer um dos itens seguintes:

- Um evento de um conector do Catalyst
- Um arquivo recebido
- Um email
- Um SNMP trap

Depois de configurar um disparador de arquivo ou de email, você pode criar o conteúdo XML. O conteúdo XML inicia os processos configurados do CA Process Automation com os parâmetros dos aplicativos externos. O conteúdo XML pode ser colocado em um arquivo e armazenado no diretório configurado ou enviado como um email à conta configurada. O disparador chama o processo especificado no conteúdo XML quando os critérios especificados forem atendidos. A instância do processo chamada pelo disparador também preenche os conjuntos de dados do processo com os valores especificados no conteúdo XML.

Depois que você configura um disparador de SNMP trap no CA Process Automation, os aplicativos externos podem enviar SNMP traps para o CA Process Automation. Quando o CA Process Automation recebe um SNMP trap que corresponde às IDs de objeto (OIDs) e ao filtro dos valores da carga, o processo configurado é iniciado. O conjunto de dados do processo disparado recebe as informações do trap.

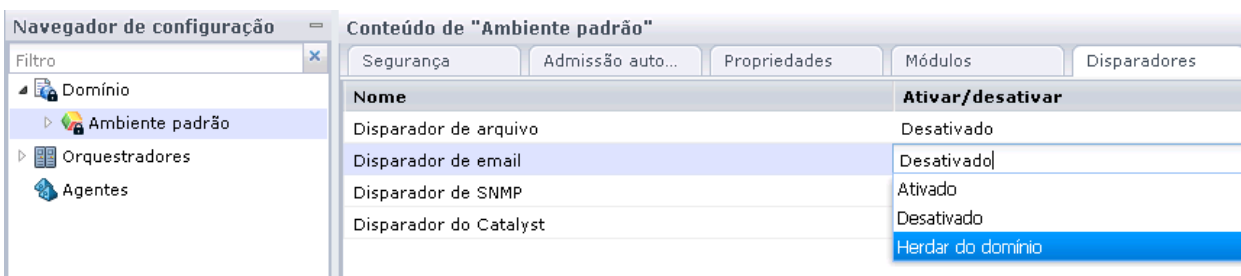
Depois que você configurar uma assinatura de evento do Catalyst, conectores externos do Catalyst poderão enviar eventos ao CA Process Automation. Quando o CA Process Automation receber um evento do Catalyst que corresponder ao filtro, o processo configurado será iniciado com as propriedades do evento disponíveis no conjunto de dados do processo.

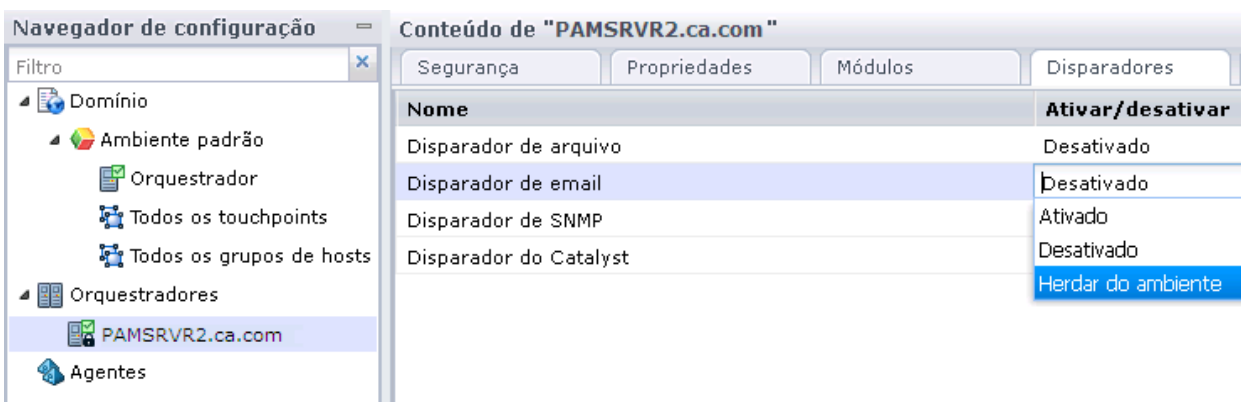
Diferente das configurações que o ambiente herda do domínio por padrão, os disparadores são desativados nos níveis do ambiente e do orquestrador por padrão. Para ativar disparadores do CA Process Automation definidos no nível do domínio, defina a herança do domínio no nível do ambiente. Em seguida, defina-a no ambiente no nível do orquestrador. Como alternativa, você pode substituir os valores herdados e configurar os valores de disparador nos níveis do ambiente e orquestrador.

Usar a seguinte abordagem para implementar disparadores:

1. Configure os disparadores no nível do Domínio. Essas configurações não são herdadas por padrão. Configure os disparadores somente se desejar aceitar o início do processo de aplicativos externos e somente para os tipos de disparador que deseja receber.

2. No nível do ambiente, em que o status do disparador é Desativado, execute uma das seguintes ações:

   - Deixe desativado para os tipos de disparador que não são aplicáveis.
   - Altere o status para Herdar do domínio para os Ambientes em que a configuração de Domínio é aplicável.
   - Altere o status para Ativado e configure os disparadores nesse nível, quando necessário.

3. No nível do Orquestrador, em que o status do disparador é Desativado, execute uma das seguintes ações:

   - Deixe desativado para os tipos de disparador que não são aplicáveis.
   - Altere o status para Herdar do ambiente. Se você selecionar essa opção, os valores serão coletados do ambiente no tempo de execução se os disparadores estiverem definidos no nível do ambiente. Caso contrário, os valores definidos no nível do Domínio serão usados.
   - Altere o status para Ativado e edite as propriedades.

4. O CA Process Automation pesquisa o diretório, a conta de email e a porta que foram configurados para o conteúdo que corresponde aos critérios do disparador.
   - Os aplicativos externos criam a entrada para os disparadores configurados:
     - Para um disparador de arquivo ou email, eles criam o conteúdo XML válido. O conteúdo XML especifica o caminho para o início do processo, as credenciais, a hora de início e os valores do parâmetro de inicialização.
     - Para um disparador de SNMP trap, uma SNMP trap válida é enviada para a porta 162 com valores que correspondem aos critérios configurados.
   - Os aplicativos externos enviam disparadores para o CA Process Automation como parte do processamento de automação.
5. O CA Process Automation processa o novo conteúdo e inicia o processo configurado do CA Process Automation com os valores passados pelo aplicativo externo.
6. Monitore a instância do processo chamada pelo disparador enviado do processo externo. Você pode monitorar o processo em execução por meio da exibição de processos. Você pode exibir os valores passados pelo disparador na página que contém as variáveis do conjunto de dados para o tipo de disparador associado.

Configurar propriedades do disparador do Catalyst no nível do domínio

Os direitos de administrador de domínio permitem configurar as propriedades do acionador do Catalyst no nível do domínio. Com as propriedades herdadas do acionador do Catalyst, o produto pode iniciar processos quando recebe um evento do Catalyst.

O disparador do Catalyst oferece suporte a uma lista de assinaturas, cada uma referenciando um conector do Catalyst com um filtro. Quando o produto recebe um evento correspondente do conector do Catalyst, ele inicia o processo especificado.

É possível configurar as propriedades do acionador do Catalyst em nível de domínio.

Observação: esse procedimento mostra exemplos de configuração de um acionador do Catalyst para iniciar um processo quando o Microsoft System Center Operations Manager cria ou atualiza um objeto de alerta. As propriedades do objeto de alerta estão disponíveis como variáveis do processo.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Acionadores.
3. Clique com o botão direito do mouse no Acionador do Catalyst e clique em Editar.
4. Na caixa de diálogo Acionador do Catalyst, clique em Adicionar parâmetro .

5. Na janela Assinaturas do Catalyst, clique na guia MDR e, em seguida, preencha os campos, conforme apropriado.
6. Verifique se suas entradas se parecem com o seguinte exemplo:
7. Clique na guia Assinatura e preencha os campos, conforme apropriado.
8. Verifique se suas entradas se parecem com o seguinte exemplo:
9. Clique na guia Filtro e preencha os campos, conforme apropriado.

10. Verifique se suas entradas se parecem com o seguinte exemplo:

Assinaturas do Catalyst

Assinatura | MDR | Filtro | Segurança

☑ Criar

☑ Atualizar

☐ Excluir

entitytype

Alert

tipo de item

☐ recorrente

id

updatedAfter

17-dez-2013 12:00:00

11. Clique na guia Segurança do Catalyst.
12. Digite as credenciais nos campos Nome de usuário e Senha.
13. Para cada requisição a adicionar, clique no botão Adicionar parâmetro, sob Requisições, e, em seguida, preencha os campos Nome da requisição e Valor da requisição.
14. Para cada senha a adicionar, clique no botão Adicionar parâmetro, sob Requisições de senha, e, em seguida, preencha os campos Nome da requisição e Valor da requisição.
15. Clique em Salvar e fechar.

    O produto adicionará a assinatura que você definiu à lista Assinatura. Para editar a definição, realce a entrada e, em seguida, clique em Editar.
16. Clique em Salvar.
17. Selecione Domínio e clique em Desbloquear.

Configurar as propriedades do acionador de arquivo no nível do domínio

Os direitos de administrador de domínio permitem configurar as propriedades do acionador de arquivo no nível do domínio. Herança *não* é o padrão. Portanto, para usar as configurações definidas no nível do domínio, defina a opção Herdar do domínio no nível do ambiente e defina a opção Herdar de ambiente no nível do orquestrador.

Ao usar os acionadores de arquivo para iniciar processos, o orquestrador procura o diretório de entrada especificado para os novos arquivos em intervalos configurados. O produto analisa o conteúdo de cada arquivo que corresponde ao padrão do nome do arquivo de entrada especificado e dispara o processo especificado. Depois que dispara o processo, o produto move o arquivo para o Diretório processado especificado. Se o produto não conseguir iniciar o processo, move o arquivo de disparo e um arquivo .err para o Diretório de erro especificado. O arquivo .err descreve o motivo pelo qual o acionador falhou.

Observação: se um novo arquivo tiver o mesmo nome que um arquivo existente, substituirá o arquivo antigo.

Antes de configurar as propriedades do acionador de arquivo, é preciso criar os seguintes diretórios:

- Um Diretório de entrada com as permissões de gravação necessárias para aceitar os arquivos de disparo. Para permitir o disparo remoto, considere a possibilidade de associar o diretório com uma pasta FTP.
- Um Diretório processado para receber a saída processada com êxito.
- Um Diretório de erro para as saídas que não podem ser processadas.

Se eles não existirem, o produto criará os diretórios.

É possível configurar as propriedades do acionador de arquivo em nível de domínio.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Acionadores, clique com o botão direito do mouse em Acionador de arquivo e clique em Editar.
3. Na caixa de diálogo Acionador de arquivo, preencha os campos, conforme apropriado.

4. Verifique se suas entradas são válidas. O exemplo a seguir contém entradas válidas.

Diretório de entrada:
./triggers
Diretório processado:
./triggeroutput/processed
Diretório de erro:
./triggeroutput/error
Timer de estabilidade (segundos):
2
Frequência (em segundos)
30
Padrão do nome do arquivo de entrada:
.*.prg

5. Clique em Salvar e fechar.
6. Clique em Salvar.
7. Selecione Domínio e clique em Desbloquear.

Configurar propriedades do disparador de email no nível do Domínio

Os direitos de administrador de domínio permitem configurar as propriedades do acionador de email no nível do domínio. As propriedades do acionador de email permitem o disparo dos processos apenas quando forem herdadas ou configuradas em níveis inferiores. Para obter a herança, configure a opção Herdar do domínio no nível do ambiente e configure a opção Herdar do ambiente no nível do orquestrador.

Quando ativo, o acionador de email pesquisa a conta de email (configurada como Nome de usuário e Senha) para localizar emails. Se o corpo do email ou o anexo possuir um conteúdo XML válido, o produto irá processá-lo. Os parâmetros que o produto cria na instância do processo disparado dependem do fato de o email possuir ou não um conteúdo XML válido.

Antes de configurar as propriedades do acionador de email, execute as tarefas a seguir:

- Crie uma conta de email dedicada a receber emails que disparam processos.
- Verifique se o serviço IMAP está ativado no servidor de email identificado como o servidor de entrada de email.

  Se o seu servidor de email corporativo restringir a ativação do serviço IMAP, crie um servidor de email proxy com o IMAP ativado. Especifique o servidor proxy como o servidor de entrada de email. Em seguida, configure seu servidor de email corporativo para encaminhar os emails endereçados para a conta de usuário configurada para o servidor de email proxy.
- (Opcional) Crie um processo padrão do orquestrador de domínio e salve-o no caminho do manipulador de processo padrão. O produto usa o processo padrão apenas quando o email não possuir um conteúdo XML válido. Nesse caso, o processo padrão inicia e preenche as seguintes variáveis na página SMTP no conjunto de dados do processo:

  senderAdd

  Identifica o endereço de email do remetente.

  senderTime

  Identifica a hora do servidor de email em que o email foi enviado.

  MailBody

  Contém o conteúdo completo do email.

  O processo padrão determina qualquer ação adicional.

É possível configurar as propriedades do acionador de email em nível de domínio.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Acionadores, clique com o botão direito do mouse em Acionador de email e clique em Editar.
3. Na caixa de diálogo Acionador de email, na guia Propriedades gerais, preencha os campos, conforme apropriado.

   Processo padrão do disparador (Orquestrador somente)

   Especifica como tratar emails que têm um conteúdo XML inválido no corpo da mensagem ou em um anexo.

   Valores:

   - **Em branco** - Ignorar os emails sem um conteúdo de acionador XML válido.
   - O caminho completo do processo que o orquestrador de domínio iniciará. (Um processo padrão pode ser definido para cada Orquestrador).

Servidor de email IMAP

Especifica o nome do host ou endereço IP do servidor de email que recebe os emails de entrada. A pasta Caixa de entrada para a conta de email configurada é pesquisada quanto a novos emails. Esse servidor deve ter o protocolo IMAP ativado. O Acionador de email não oferece suporte ao POP3.

Porta do servidor IMAP

Se a porta TCP padrão para um servidor IMAP for usada, digite 143. Se uma porta não padrão for usada ou a comunicação segura estiver configurada em uma porta diferente, obtenha do administrador a porta correta para entrar.

Nome de usuário

Especifica o nome de usuário usado para conectar ao servidor de entrada de email. Observe os requisitos de seu servidor IMAP ao determinar se digitará o endereço de email completo ou o alias como o nome do usuário. O nome de usuário pamadmin@ca.com é um exemplo de um endereço completo; pamadmin é o alias.

Observação: o Microsoft Exchange Server aceita tanto o endereço de email completo quanto o alias.

Senha

Especifica a senha associada ao nome de usuário especificado.

Intervalo entre processamentos de email (segundos)

A frequência corresponde aos segundos em que o CA Process Automation pesquisa o servidor IMAP quanto a novos emails de entrada na conta especificada. O nome de usuário e a senha especificam a conta.

Padrão:

2

Salvar anexos de email no banco de dados

Especifica se é necessário salvar anexos de emails que disparam os processos do CA Process Automation no banco de dados.

- Selecionado: o CA Process Automation salva os anexos de emails no banco de dados do CA Process Automation e preenche o conjunto de dados do processo iniciado com informações relevantes dos anexos.
- Limpo: o CA Process Automation não salva os anexos de email.

Servidor de email SMTP de saída

Especifica o nome do servidor de email SMTP de saída. Quando um email de disparo com conteúdo XML válido for recebido na conta configurada do servidor de email IMAP, um email de confirmação é retornado. O email de confirmação é retornado ao remetente pelo servidor SMTP de saída.

Porta do servidor SMTP

Especifica a porta do servidor de email de saída.

Padrão:

25

Usar conexão SMTP segura

Especifica se é necessário utilizar uma conexão segura para se conectar ao servidor de email SMTP.

- **Marcado** - O servidor de email permite uma conexão segura com o servidor de email SMTP.
- **Desmarcado** - O servidor de email não permite uma conexão segura.

Padrão:

Desmarcado

4. Clique em Salvar e fechar.
5. Clique em Salvar.
6. Selecione Domínio e clique em Desbloquear.

Configurar propriedades do acionador de SNMP no nível do Domínio

Um administrador com direitos de administrador de domínio pode configurar as propriedades do acionador de SNMP no nível do domínio. Quando herdadas, as propriedades do acionador de SNMP ativam os Processos para serem disparados após o recebimento de uma SNMP trap.

Antes de começar a configurar as propriedades do acionador de SNMP, verifique se a porta 162 está acessível para o CA Process Automation. Modifique a porta de escuta dos SNMP traps no arquivo de propriedades do CA Process Automation se você usar uma porta alternativa.

Siga estas etapas:

1. Clique na guia Configuração, selecione Domínio e clique em Bloquear.
2. Clique na guia Acionadores, clique com o botão direito do mouse em Acionador de SNMP e clique em Editar.
3. Clique em Adicionar parâmetro.
4. Na janela Acionador de SNMP, preencha os campos de Filtro de trap, conforme apropriado.

5. Verifique se suas entradas são válidas.

   O exemplo de filtro a seguir aceita os SNMP traps de qualquer host que possui as seguintes características:

   - Um endereço IP entre 138.42.7.1 e 138.42.7.254 com uma OID que começa com 1.3.6.1.4.1.[x.x.x.x.x]
   - Pelo menos um valor da carga que corresponde à sequência de caracteres literal "carga de teste para o acionador."

   Quando o produto recebe um SNMP trap que corresponde a esses critérios, dispara o processo RunProcess1 no caminho/teste.

   Disparador de SNMP

   Filtro de trap

   Descrição:
   Test Process1
   Endereço IP de origem
   138.42.7.0/24
   OID de trap
   1.3.6.1.4.*
   Correspondência de carga:
   .*
   Caminho do processo
   /Test/RunProcess1

   Cancelar Salvar e fechar

6. Clique nos botões Mover para cima e Mover para baixo, conforme apropriado, para organizar a lista por ordem de precedência. Cada filtro tem precedência sobre os filtros listados abaixo dele.

   Exibir

1	Test Process1
2	Test Process2

7. Clique em Salvar.

8. Selecione Domínio e clique em Desbloquear.

Mais informações:

Alterar a porta de escuta de SNMP Traps (na página 325)

Alterar a porta de escuta de SNMP Traps

Por padrão, o CA Process Automation escuta na porta 162 as SNMP traps projetadas para iniciar processos do CA Process Automation. Se você fechou a porta 162 no seu site e configurou uma alternativa, altere a configuração do CA Process Automation para essa porta no arquivo OasisConfig.properties. Em seguida, reinicie o serviço do orquestrador.

É possível alterar a porta em que o CA Process Automation escuta as SNMP traps.

Siga estas etapas:

1. Faça o logon no servidor em que o Orquestrador de domínio está configurado.
2. Vá até a seguinte pasta ou diretório:

   `dir_instalação/server/c2o/.config/`
3. Abra o arquivo OasisConfig.properties
4. Altere o valor na seguinte linha de 162 até o número da porta que você está usando para SNMP traps.

   `oasis.snmptrigger.service.port=162`
5. Salve o arquivo.
6. Reinicie o serviço do orquestrador.
   a. Interrompa o orquestrador (na página 193).
   b. Inicie o orquestrador (na página 194).

   Assim que o serviço for reiniciado, o CA Process Automation começará a escutar na porta configurada. O CA Process Automation escuta novos SNMP traps que atendam aos critérios configurados no disparador de SNMP.

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Capítulo 14: Gerenciar recursos de usuário

É possível gerenciar recursos para usuários, orquestradores e agentes na paleta Gerenciar recursos de usuário da guia Configuração.

A paleta Gerenciar recursos de usuário contém três pastas em Repositório:

- Recursos do agente
- Recursos do orquestrador
- Recursos do usuário, que inclui a subpasta, VBS_Resources.

  Observação: é possível adicionar subpastas apenas na pasta Recursos do usuário.

Os usuários que recebem a permissão Configuration_User_Resources na diretiva do Navegador de configuração no CA EEM podem gerenciar recursos na pasta Recursos do usuário. No entanto, apenas os usuários que também receberem as permissões Domain_Administrator da diretiva do Domínio poderão acessar as pastas Recursos do orquestrador e Recursos do agente. Os integrantes do grupo padrão PAMAdmins têm essas duas permissões.

Esta seção contém os seguintes tópicos:

Sobre o gerenciamento de recursos do usuário

O gerenciamento de recursos exige permissões específicas para várias atividades. Os usuários que pertencem ao grupo padrão PAMAdmins (o grupo com todas as permissões) podem executar qualquer atividade do gerenciamento de recursos.

Os usuários em grupos personalizados que possuem diretivas personalizadas devem ter acesso básico e uma ou ambas as seguintes permissões:

Diretiva de ambiente PAM40: Environment_Configuration_Admin (Administrador de configuração)

Os usuários com permissões de Environment_Configuration_Admin (Administrador de configuração) podem carregar, modificar ou excluir qualquer tipo de arquivo dos Recursos do usuário. Por exemplo:

- Um arquivo JAR para ser usado com o operador Chamar o Java
- Um script para ser usado com o operador Executar o script
- Uma imagem

Diretiva do domínio PAM40: Domain_Admin (Administrador)

Usuários com permissões de Domain_Admin (Administrador) podem executar as seguintes tarefas:

- Adicionar recursos à pasta Recursos do orquestrador ou à pasta Recursos do agente
- Editar o conteúdo de um recurso e readicioná-lo; atualizar os campos descritivos
- Excluir um recurso do orquestrador ou recurso do agente carregado anteriormente

Observação: os procedimentos para edição e exclusão de recursos do orquestrador e do agente são semelhantes aos procedimentos para edição e exclusão de recursos do usuário.

As diferenças entre os recursos do usuário e os recursos do agente ou do orquestrador são as seguintes:

Recursos do usuário

- Após uma reinicialização, o caminho da classe do agente ou do orquestrador não inclui os recursos que foram carregados nos Recursos do usuário.
- É possível criar subpastas dentro da pasta Recursos do usuário.
- Você não precisa de direitos Domain_Admin (Administrador).

Recursos do agente e recursos do orquestrador

- Após uma reinicialização, o caminho da classe do agente ou do orquestrador inclui os recursos que foram carregados nos recursos do agente e nos recursos do orquestrador.

- Não é possível criar subpastas dentro das pastas Recursos do agente e Recursos do orquestrador.
- Você precisa de direitos Domain_Admin (Administrador).

Como implantar drivers JDBC para operadores Banco de dados

É possível instalar drivers JDBC para os operadores de banco de dados durante a instalação ou depois que o CA Process Automation estiver instalado. Apenas os processos com operadores de banco de dados exigem um driver JDBC.

Durante a instalação, os drivers JDBC carregados na instalação do software de terceiros são exibidos, mas não selecionados. Você pode selecionar os drivers JDBC para MySQL, Microsoft SQL Server e Oracle. Além disso, você pode adicionar outros arquivos JAR copiados em um diretório local.

Após a instalação, é possível carregar arquivos JAR que contêm drivers JDBC para operadores Banco de dados usando a paleta Gerenciar recursos de usuário na guia Configuração. O CA Process Automation implanta os arquivos JAR carregados em orquestradores ou agentes, dependendo da pasta que você selecionar durante o upload. Consulte os tópicos a seguir para obter mais informações:

- Carregar recursos do orquestrador (na página 329).
- Carregar Recursos do agente (na página 331).

Carregar recursos do orquestrador

Após a instalação, a pasta Recursos do orquestrador exibe apenas os arquivos JDBC JAR que foram adicionados durante a instalação. Depois de usar a paleta Gerenciar recursos de usuário para atualizar a pasta Recursos do orquestrador, a pasta Recursos do orquestrador também exibe os arquivos JAR carregados.

É possível carregar um arquivo JAR para a pasta Recursos do orquestrador no Orquestrador de domínio. Quando você reiniciar o orquestrador de domínio, o CA Process Automation implantará o arquivo no orquestrador de domínio. O orquestrador de domínio espelha (copia) o arquivo no intervalo de espelhamento configurado, após o qual reiniciam-se os outros orquestradores. Quando os orquestradores reiniciam, o arquivo espelhado fica disponível para uso.

Observação: o espelhamento se aplica a todos os orquestradores no domínio. Para orquestradores agrupados, o espelhamento se aplica a todos os nós de cada agrupamento.

Siga estas etapas:

1. Clique na guia Configuração.

2. Clique na paleta Gerenciar recursos de usuário e expanda a pasta Repositório.
3. Selecione a pasta Recursos do orquestrador.
4. Clique em Novo.

   O painel Adicionar novo recurso: Sem título é aberto.
5. Forneça os detalhes do upload nos campos a seguir conforme apropriado:
   a. Digite o nome do recurso no campo Nome do recurso.

      O exemplo a seguir é uma maneira razoável de especificar o nome do recurso se você estiver fazendo upload de um driver do JDBC:

      `Driver` *`database_name`*

      database_name

      Define o nome do RDBMS. Por exemplo, driver Oracle, driver MySQL ou driver Sybase.
   b. Clique em Procurar, vá até o local onde o arquivo JAR foi salvo e selecione o arquivo de destino. Isso preenche o campo Arquivo de recurso.
   c. Selecione um nome de módulo especificado pelo usuário na lista suspensa Nome do módulo.
   d. (Opcional) Digite uma descrição do recurso no campo Descrição do recurso.
6. Verifique o que foi digitado e, em seguida, clique em Salvar.

   Uma linha com a sua entrada é exibida.

☑	Nome	Tipo de arquivo	Caminho do arquivo	Módulo
☑	Sybase Driver	jar	.c2oserverresources/lib/jconn2.jar	Sybase Driver

   O CA Process Automation copia o recurso carregado para os seguintes caminhos:

   `install_dir``/server/c2o/ext-lib`

   `install_dir``/server/c2o/.c2orepository/.c2oserverresources/lib`

   install_dir

   Define o diretório no servidor onde o orquestrador de domínio foi instalado.
7. Reinicie o Orquestrador de domínio. (Interrompa o orquestrador de domínio (na página 193) e, em seguida, inicie-o (na página 194).

   Quando o orquestrador de domínio é reiniciado, o sistema implanta todos os jars carregados nos Recursos do orquestrador de domínio. Ou seja, o CA Process Automation coloca os jars no caminho da classe do orquestrador de domínio.
8. Após o espelhamento, reinicie todos os outros orquestradores.

   O sistema implanta todos os jars carregados em todos os orquestradores. Ou seja, o sistema coloca os jars no caminho da classe dos orquestradores.

   Observação: para orquestradores agrupados, reinicie cada nó.

Carregar Recursos do agente

Usuários com permissões de administrador de domínio podem carregar recursos para a pasta Recursos do agente no orquestrador de domínio. O recurso carregado pode ser um arquivo jar, por exemplo, um driver do JDBC. Os recursos do agente carregados são espelhados no intervalo de espelhamento configurado. Após o espelhamento, reinicie os agentes. Agentes reiniciados podem usar os recursos do agente carregados.

Siga estas etapas:

1. Navegue para o CA Process Automation e efetue logon (na página 18).
2. Clique na guia Configuração.
3. Clique na paleta Gerenciar recursos de usuário e expanda a pasta Repositório.
4. Selecione a pasta Recursos do agente e clique em Novo.

   O painel Adicionar novo recurso: Sem título é aberto.

5. Forneça os detalhes do upload, usando as descrições de campo abaixo, conforme necessário.

   a. Digite o nome do recurso no campo Nome do recurso.

      Se estiver carregando um driver do JDBC, digite driver *database_name*; onde *database_name* é o RDBMS (Relational Database Management System - Sistema de Gerenciamento de Banco de Dados Relacional). Por exemplo, driver Oracle, driver MySQL ou driver Sybase.

   b. Clique em Procurar, vá até o local onde você salvou o arquivo jar e selecione o arquivo de destino.

      Isso preenche o campo Arquivo de recurso com o arquivo e o seu caminho.

   c. (Opcional) Selecione um nome de módulo definido pelo usuário na lista suspensa Nome do módulo.

   d. (Opcional) Digite uma descrição significativa no campo Descrição.

6. Verifique sua entrada. Em seguida, clique em Salvar.

   Uma linha com a sua entrada é exibida.

   O CA Process Automation copia os recursos carregados, por exemplo, um driver do JDBC, no seguinte caminho, onde *install_dir* é o diretório no servidor onde o orquestrador de domínio estava instalado.

   ```
   install_dir/server/c2o/.c2orepository/.c2oagentresources/lib/drivers/jars
   ```

7. Após a conclusão do espelhamento, reinicie os agentes onde precisa dos arquivos jar carregados. Os arquivos jar são colocados no caminho de classe dos agentes reiniciados.

   Observação: consulte o tópico Como iniciar ou interromper um agente para obter detalhes sobre a reinicialização de agentes.

Carregar Recursos do usuário

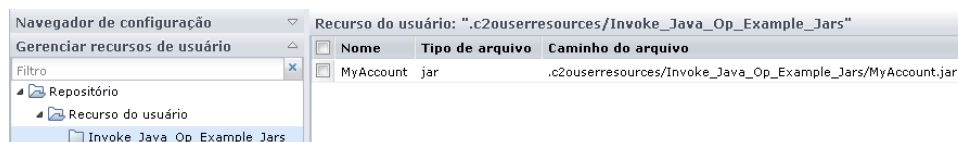
O upload envolve criar uma pasta na pasta Recursos do usuário e navegar até o recurso a ser carregado. O CA Process Automation adiciona o recurso à estrutura de árvore de Recursos do usuário e carrega o recurso.

Veja os procedimentos a seguir:

- Adicionar um recurso a Recursos do usuário (na página 332).
- Excluir um recurso de Recursos do usuário (na página 333).
- Modificar um recurso em Recursos do usuário (na página 334).

Observação: para modificar o caminho do recurso, exclua o recurso e adicione-o novamente com outro caminho.

Recurso para executar um exemplo do operador Chamar o Java

O processo de instalação adiciona um recurso à pasta Recurso do usuário no Repositório na paleta Gerenciar recursos de usuário, na guia Configuração. O arquivo JAR, MyAccount.jar, está localizado na pasta Invoke_Java_Op_Example_jars. Você pode usar o arquivo MyAccount.jar para executar o exemplo de Java fornecido no campo Required Main Method do operador Chamar o Java.

Adicionar um recurso a Recursos do usuário

Os usuários com permissões de nível administrativo podem adicionar scripts à pasta Recursos do usuário no Repositório global. Os recursos do usuário carregados são espelhados pelo produto no intervalo configurado para outros orquestradores e agentes no domínio. Os orquestradores e agentes podem acessar recursos do usuário por referência.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique na paleta Gerenciar recursos de usuário.
3. Expanda a pasta Repositório e, em seguida, expanda a pasta Recurso do usuário.
4. Selecione a pasta Recurso do usuário ou uma subpasta e clique em Novo.

5. Preencha os campos no painel Adicionar novo recurso, conforme apropriado.
6. Verifique o que foi digitado e, em seguida, clique em Salvar.

   A lista no painel Recurso do usuário exibe o nome, tipo, caminho, módulo e descrição do arquivo carregado.

O produto copia os recursos do usuário carregados no seguinte caminho:

`install_dir/server/c2o/.c2orepository/.c2ouserresources/...`

install_dir

Define o diretório no servidor onde o orquestrador de domínio foi instalado.

O produto cria subpastas conforme necessário para manter o caminho da pasta Recursos do usuário até o recurso.

Mais informações:

Carregar descritores do Catalyst (na página 273)

Excluir um recurso de Recursos do usuário

Você poderá excluir um recurso, como um script ou arquivo jar, que adicionou à pasta Recursos do usuário.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique na paleta Gerenciar recursos de usuário.
3. Expanda a pasta Repositório. Expanda a pasta Recursos do usuário.
4. Clique na pasta em que o recurso está localizado.
5. Selecione a linha que exibe o nome do recurso para excluir e, em seguida, clique em Excluir.

Observação: quando você excluir o último recurso de uma subpasta de Recursos do usuário, essa subpasta também será excluída.

Modificar um recurso em Recursos do usuário

É possível modificar um recurso das maneiras a seguir:

- É possível alterar o texto em qualquer campo exibido, exceto no Caminho do recurso. Esta ação é possível se você selecionar Substituir arquivo ou não.
- É possível carregar um recurso editado (como um script ou arquivo JAR), adicionado anteriormente a Recursos do usuário. Esta ação somente é possível se você selecionar Substituir arquivo.

Siga estas etapas:

1. Clique na guia Configuração.
2. Clique na paleta Gerenciar recursos de usuário.
3. Expanda a pasta Repositório e, em seguida, expanda a pasta Recursos do usuário.
4. Clique na pasta em que o recurso reside.
5. Clique com o botão direito do mouse na linha que exibe o nome do recurso a modificar e selecione Editar.

   A página Recurso é aberta.
6. (Opcional) Modifique as informações do recurso. É possível editar os campos a seguir:
   - Nome do recurso
   - Nome do módulo
   - Descrição do recurso
7. Defina a caixa de seleção Substituir arquivo como a seguir:
   - Se as alterações do recurso forem *apenas* campos atualizados na página Recurso, desmarque a caixa de seleção Substituir arquivo e clique em Salvar.
   - Se você atualizou sua cópia local do arquivo de recurso e deseja fazer upload das atualizações:
     a. Selecione Substituir arquivo.
     b. Clique em Procurar.
     c. Navegue até o arquivo atualizado e clique em Abrir.
     d. Clique em Salvar.

   A pasta Recursos do usuário agora contém o arquivo atualizado. A página Recursos contém texto para qualquer campo modificado.

Capítulo 15: Auditorar ações do usuário

O CA Process Automation fornece trilhas de auditoria para rastrear e registrar a atividade de objetos de configuração (domínio, ambientes, agentes e orquestradores) e de objetos de biblioteca (pastas e objetos de automação). Um administrador de Domínio pode visualizar a trilha de auditoria do Domínio. Um administrador de configuração do Ambiente pode visualizar a trilha de auditoria de um Ambiente. Um usuário final com a permissão Usuário do ambiente pode exibir a trilha de auditoria de um objeto.

Esta seção contém os seguintes tópicos:

Visualizar a trilha de auditoria do Domínio

Os administradores podem exibir a trilha de auditoria do domínio.

A trilha de auditoria do domínio monitora as seguintes ações:

- Domínio bloqueado ou desbloqueado.
- Propriedade de domínio alterada.
- Orquestrador de domínio alterado.
- Ambiente criado, excluído, bloqueado, desbloqueado ou renomeado.
- Orquestrador adicionado, excluído ou renomeado.
- Agente adicionado, excluído ou renomeado.
- A referência ao agente foi atribuída ao touchpoint 'nome-do-touchpoint'.

O exemplo a seguir mostra a trilha de auditoria para atribuir um touchpoint a um agente. Duas das colunas estão ocultas.

Conteúdo de "Dominio"

Segurança | Propriedades | Módulos | Disparadores | Trilhas de audit...

Nome do objeto	Última atualização	Nome de usuário	Tipo de ação	Descrição
Entorno predeterminado	10-Dec-2013 21:45:15	pamadmin	Bloqueado	O ambiente foi bloqueado com êxito.
Dominio	10-Dec-2013 20:39:40	pamadmin	Bloqueado	O orquestrador de domínio foi bloqueado com êxito.
WIN-EQS1JRM3VFN.ca.com	10-Dec-2013 21:45:01	pamadmin	Bloqueado	O agente foi bloqueado com êxito.

Siga estas etapas:

1. Selecione a guia Configuração.
2. Na paleta Navegador de configuração, selecione o nó Domínio.
3. No painel Conteúdo, clique na guia Trilhas de auditoria.

   A guia Trilhas de auditoria exibe as seguintes informações para todos os registros:

   - Nome do objeto
   - Última atualização
   - Nome de usuário
   - Tipo de ação
   - Descrição

4. (Opcional) Para classificar as trilhas de auditoria em uma coluna específica, selecione Classificação crescente ou Classificação decrescente na lista suspensa da coluna de destino.

   Por exemplo, para fazer auditoria de um usuário específico, selecione uma opção de classificação na lista suspensa da coluna Nome do usuário e, em seguida, role até o registro apropriado.

5. (Opcional) Para alterar o número de registros que o produto exibe em uma página, selecione um valor na lista suspensa Linhas em cada página.
6. Examine os registros na trilha de auditoria.

   Se os registros de auditoria incluírem várias páginas, use os botões de navegação da barra de ferramentas para exibir a primeira página, a página anterior, a próxima página ou a última página.

Visualizar a trilha de auditoria de um Ambiente

Com direitos de acesso de administrador de configuração, você pode exibir a trilha de auditoria do ambiente.

A trilha de auditoria do ambiente monitora as seguintes ações:

- O ambiente é bloqueado ou desbloqueado. A propriedade do ambiente é alterada.
- O ambiente é criado ou excluído.
- O ambiente ou objeto no ambiente é renomeado.
- O touchpoint é adicionado, excluído ou renomeado.
- O grupo de touchpoints é adicionado ou excluído.
- O grupo de hosts é adicionado ou excluído.

Siga estas etapas:

1. Clique na guia Configuração.
2. Na paleta Navegador de configuração, expanda o nó Domínio e selecione o ambiente a ser auditado (por exemplo, o ambiente padrão).
3. No painel Conteúdo, clique na guia Trilhas de auditoria.

   A guia Trilhas de auditoria exibe as seguintes informações para todos os registros:

   - Nome do objeto
   - Última atualização
   - Nome de usuário
   - Tipo de ação
   - Descrição
4. (Opcional) Para classificar as trilhas de auditoria em uma coluna específica, selecione Classificação crescente ou Classificação decrescente na lista suspensa da coluna de destino.

   Por exemplo, para fazer auditoria de um usuário específico, selecione uma opção de classificação na lista suspensa da coluna Nome do usuário e, em seguida, role até o registro apropriado.
5. (Opcional) Para alterar o número de registros que o produto exibe em uma página, selecione um valor na lista suspensa Linhas em cada página.
6. Examine os registros na trilha de auditoria.

   Se os registros de auditoria incluírem várias páginas, use os botões de navegação da barra de ferramentas para exibir a primeira página, a página anterior, a próxima página ou a última página.

Visualizar a trilha de auditoria de um Orquestrador

Com permissões de leitura em um objeto de configuração, você pode exibir a trilha de auditoria associada. Direitos de acesso são necessários para exibir a trilha de auditoria dos objetos de configuração que incluem Usuário do ambiente e Exibir navegador de configuração.

A trilha de auditoria do orquestrador monitora as seguintes ações:

- O orquestrador é bloqueado ou desbloqueado.
- A propriedade do orquestrador é alterada.
- O orquestrador é colocado em quarentena ou não é colocado em quarentena.
- O orquestrador é mapeado para um touchpoint ou tem o mapeamento removido de um touchpoint.
- O orquestrador é renomeado.

Siga estas etapas:

1. Clique na guia Configuração.
2. Na paleta Navegador de configuração, expanda o nó Orquestradores e selecione o orquestrador de destino.
3. No painel Conteúdo, clique na guia Trilhas de auditoria.

   A guia Trilhas de auditoria exibe as seguintes informações para todos os registros:

   - Nome do objeto
   - Última atualização
   - Nome de usuário
   - Tipo de ação
   - Descrição
4. (Opcional) Para classificar as trilhas de auditoria em uma coluna específica, selecione Classificação crescente ou Classificação decrescente na lista suspensa da coluna de destino.

   Por exemplo, para fazer auditoria de um usuário específico, selecione uma opção de classificação na lista suspensa da coluna Nome do usuário e, em seguida, role até o registro apropriado.
5. (Opcional) Para alterar o número de registros que o produto exibe em uma página, selecione um valor na lista suspensa Linhas em cada página.
6. Examine os registros na trilha de auditoria.

   Se os registros de auditoria incluírem várias páginas, use os botões de navegação da barra de ferramentas para exibir a primeira página, a página anterior, a próxima página ou a última página.

Visualizar a trilha de auditoria de um Agente

Com permissões de leitura em um objeto de configuração, você pode exibir a trilha de auditoria associada. Direitos de acesso do CA EEM são necessários para exibir a trilha de auditoria dos objetos de configuração que incluem Usuário do ambiente e Exibir navegador de configuração.

A trilha de auditoria do agente monitora as seguintes ações:

- A categoria do operador é ativada na guia Módulos e altera um valor configurado.
- O agente é colocado em quarentena ou não é colocado em quarentena.
- O agente é bloqueado ou desbloqueado.

Siga estas etapas:

1. Clique na guia Configuração.
2. Na paleta Navegador de configuração, expanda o nó Agentes e selecione o agente de destino.
3. No painel Conteúdo, clique na guia Trilhas de auditoria.

   A guia Trilhas de auditoria exibe as seguintes informações para todos os registros:

   - Nome do objeto
   - Última atualização
   - Nome de usuário
   - Tipo de ação
   - Descrição
4. (Opcional) Para classificar as trilhas de auditoria em uma coluna específica, selecione Classificação crescente ou Classificação decrescente na lista suspensa da coluna de destino.

   Por exemplo, para fazer auditoria de um usuário específico, selecione uma opção de classificação na lista suspensa da coluna Nome do usuário e, em seguida, role até o registro apropriado.
5. (Opcional) Para alterar o número de registros que o produto exibe em uma página, selecione um valor na lista suspensa Linhas em cada página.
6. Examine os registros na trilha de auditoria.

   Se os registros de auditoria incluírem várias páginas, use os botões de navegação da barra de ferramentas para exibir a primeira página, a página anterior, a próxima página ou a última página.

Visualizar a trilha de auditoria de um Touchpoint, Grupo de Touchpoints ou Grupo de hosts

Com permissões de leitura em um objeto de configuração, você pode exibir a trilha de auditoria associada. Direitos de acesso são necessários para exibir a trilha de auditoria dos objetos de configuração que incluem Usuário do ambiente e Exibir navegador de configuração.

As trilhas de auditoria de touchpoint, grupo de touchpoints e grupo de hosts monitoram as seguintes ações:

- O touchpoint é criado.
- O agente é atribuído ao touchpoint.
- O grupo de touchpoints é criado.
- O touchpoint é adicionado a um grupo.
- O grupo de touchpoints é renomeado.
- O grupo de hosts é criado.

Siga estas etapas:

1. Clique na guia Configuração.
2. Na paleta Navegador de configuração, expanda o nó Domínio. Em seguida, expanda o nó Ambiente que contém o touchpoint de destino, o grupo de touchpoints ou o grupo de hosts.
3. Expanda o nó apropriado (Todos os Touchpoints, Todos os grupos de touchpoints ou Todos os grupos de hosts) e selecione o touchpoint, grupo de touchpoints ou grupo de hosts de destino.
4. No painel Conteúdo, clique na guia Trilhas de auditoria.

   A guia Trilhas de auditoria exibe as seguintes informações para todos os registros:

   - Nome do objeto
   - Última atualização
   - Nome de usuário
   - Tipo de ação
   - Descrição
5. (Opcional) Para classificar as trilhas de auditoria em uma coluna específica, selecione Classificação crescente ou Classificação decrescente na lista suspensa da coluna de destino.

   Por exemplo, para fazer auditoria de um usuário específico, selecione uma opção de classificação na lista suspensa da coluna Nome do usuário e, em seguida, role até o registro apropriado.

6. (Opcional) Para alterar o número de registros que o produto exibe em uma página, selecione um valor na lista suspensa Linhas em cada página.
7. Examine os registros na trilha de auditoria.

   Se os registros de auditoria incluírem várias páginas, use os botões de navegação da barra de ferramentas para exibir a primeira página, a página anterior, a próxima página ou a última página.

Visualizar a trilha de auditoria de uma pasta da biblioteca

Os administradores podem visualizar a trilha de auditoria para qualquer pasta selecionada na Biblioteca. O produto registra as seguintes ações para pastas em uma biblioteca:

- Criado
- Renomeado
- Excluído
- Criar ou excluir um objeto de automação
- Recuperar um objeto de automação ou pasta da lixeira
- Alterar permissões em uma pasta, incluindo links para as ACLs antiga e nova

Siga estas etapas:

1. Clique na guia Biblioteca e selecione um orquestrador na lista suspensa Orquestrador.
2. Vá até a pasta que contém a pasta que você deseja auditar.
3. No painel Conteúdo, clique com o botão direito do mouse na pasta que deseja auditar e selecione Propriedades.
4. No painel Propriedades, clique na guia Trilhas de auditoria.

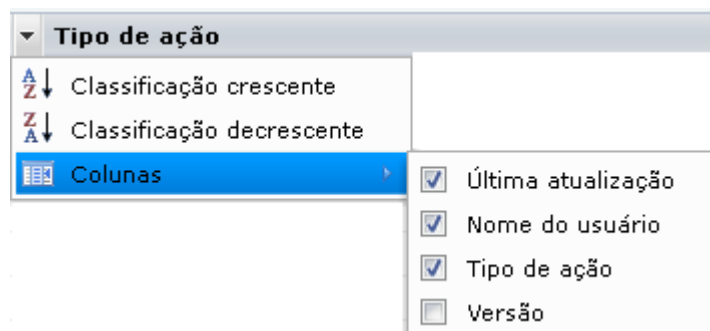
   A guia Trilhas de auditoria exibe as seguintes informações para todos os registros:

   - Última atualização
   - Nome de usuário
   - Tipo de ação
5. (Opcional) Para classificar as trilhas de auditoria em uma coluna específica, selecione Classificação crescente ou Classificação decrescente na lista suspensa da coluna de destino.

6. (Opcional) Define quais colunas o produto exibirá:

   a. Selecione Colunas na lista suspensa de qualquer cabeçalho da coluna.

   b. Desmarque (ocultar) ou marque (exibir) as caixas de seleção da coluna, conforme apropriado.

   Por exemplo, para exibir a coluna Versão, marque a caixa de seleção Versão no menu Colunas.

7. Examine os registros na trilha de auditoria.

Visualizar a trilha de auditoria para um objeto de Automação aberto

Os administradores podem exibir a trilha de auditoria para um objeto de automação aberto. O produto registra as seguintes ações para objetos de automação:

- Criar
- Excluir
- Disponibilizar e reservar
- Renomear
- Exportar e importar
- Alterar as permissões do objeto de automação, incluindo links para as ACLs antiga e nova
- Recuperar um objeto de automação da lixeira
- Alterar a versão atual designada
- Criar ou atualizar a versão da release
- Adicionar uma propriedade da versão da release
- Atualizar um objeto de automação (por exemplo, uma programação) sem reservá-lo
- Disponibilizar ou tornar indisponível um objeto Operador personalizado
- Ativar ou desativar uma programação

Siga estas etapas:

1. Clique na guia Biblioteca e selecione um orquestrador na lista suspensa Orquestrador.
2. Vá até a pasta que contém a instância do objeto de automação para auditoria.
3. No painel Conteúdo, clique com o botão direito na instância do objeto de automação de destino e, em seguida, selecione Propriedades.
4. No painel Propriedades, clique na guia Trilha de auditoria.

   A guia Trilha de auditoria exibe as seguintes informações para todos os registros:

   - Última atualização
   - Nome de usuário
   - Tipo de ação

   Observação: a coluna Versão também está disponível, mas não é exibida por padrão. Para obter mais informações, consulte a Etapa 5.
5. (Opcional) Para classificar as trilhas de auditoria em uma coluna específica, selecione Classificação crescente ou Classificação decrescente na lista suspensa da coluna de destino.

   Por exemplo, para fazer auditoria de um usuário específico, selecione uma opção de classificação na lista suspensa da coluna Nome do usuário e, em seguida, role até o registro apropriado.
6. (Opcional) Define quais colunas o produto exibirá:

   a. Selecione Colunas a partir de uma lista suspensa da coluna.

   b. Desmarque (ocultar) ou marque (exibir) as caixas de seleção da coluna, conforme apropriado.

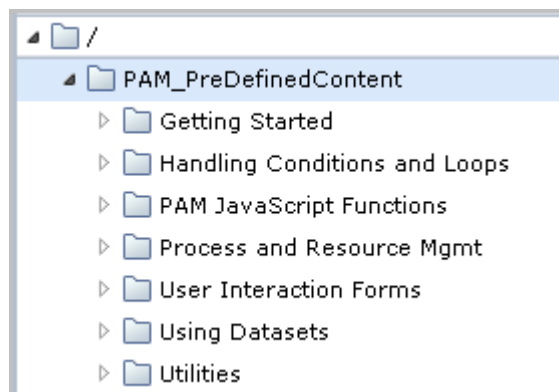
   Por exemplo, para exibir a coluna Versão, marque a caixa de seleção Versão no menu Colunas.
7. Examine os registros na trilha de auditoria.

Capítulo 16: Administrar objetos da biblioteca

Esta seção contém os seguintes tópicos:

Criar e gerenciar pastas

A biblioteca de um orquestrador de domínio do CA Process Automation instalado recentemente não contém pastas no painel de navegação da guia Biblioteca. A instalação do conteúdo pronto para uso na página principal cria pastas na biblioteca para conteúdo predefinido.

/
PAM_PreDefinedContent
Getting Started
Handling Conditions and Loops
PAM JavaScript Functions
Process and Resource Mgmt
User Interaction Forms
Using Datasets
Utilities

Normalmente, um administrador configura a estrutura de pastas para conteúdos criados por criadores de conteúdo. Os criadores salvam todos os objetos de automação nas pastas da Biblioteca. (Por padrão, os integrantes do grupo Criadores podem criar pastas.)

Observação: para um CA Process Automation atualizado, todas as pastas são migradas na estrutura anterior com seu conteúdo.

Configurar pastas para criação

Você pode usar o processo a seguir para configurar as pastas:

1. Planejar a estrutura de pastas (na página 346).
2. Criar pastas (na página 348).
3. Conceder acesso à pasta (na página 348).

Planejar a estrutura de pastas

Uma das suas primeiras decisões como um novo administrador do CA Process Automation é como organizar e usar as pastas na guia Biblioteca. A estrutura de pastas pode ter a profundidade que você considerar prática.

Para facilitar a tarefa de preparação para a exportação, configure uma estrutura de pastas semelhante a esta antes que o trabalho de criação seja iniciado. Ou seja, no nível raiz da biblioteca, crie uma pasta para cada processo que você deseja automatizar. Em cada pasta em nível de processo, crie uma pasta em nível de release usando suas próprias convenções de nomenclatura para a primeira versão da release. Se você criar atualizações para um processo, poderá adicionar novas pastas às versões de release posteriores.

```
/ (pasta raiz)
Processo automatizado 1
   Versão da release 1
   Versão da release 2
Processo automatizado 2
   Versão da release 1
   Versão da release 2
```

Quando você implanta a primeira versão da release do primeiro processo que você automatizou, exporta a pasta da versão da release, que contém todos os objetos contidos nessa release.

Considere as seguintes abordagens para a criação de uma estrutura de pastas:

- Crie a estrutura da exportação no início e use a pasta da versão da release como a pasta de trabalho. Em seguida, os criadores de conteúdo criam, atualizam e testam objetos na pasta da versão da release ou em uma de suas subpastas. A estrutura de pastas criada aqui e exportada será reproduzida no ambiente de produção durante a importação.
- Crie pastas de trabalho. Em seguida, quando a primeira versão da release de um processo estiver pronta para a implantação, crie a pasta de exportação e preencha-a com os objetos que fazem parte da versão da release.
- Abordagem híbrida. Crie a estrutura de exportação e use a pasta de exportação para a próxima versão da release como a pasta de trabalho, mas mantenha os objetos que são compartilhados entre processos em uma pasta diferente em nível de raiz. Por exemplo, vários processos podem compartilhar conjuntos de dados nomeados e subprocessos específicos. Calendários podem ser compartilhados entre programações. Programações globais podem ser compartilhadas. Em seguida, como parte da preparação para exportação, copie os objetos necessários da pasta de objetos compartilhados para a pasta de exportação.

Observação: se você exportar uma pasta com caminhos absolutos, toda a estrutura de pastas da pasta de exportação será replicada no ambiente de produção quando conteúdos forem importados.

Criar pastas

Crie uma pasta no painel esquerdo da guia Biblioteca. O painel esquerdo é o painel de navegação para a biblioteca. A pasta contém o conteúdo que os criadores de conteúdo criam com os objetos de automação. Todos os objetos que oferecem suporte a um determinado processo automatizado devem estar na mesma pasta ou na mesma estrutura de pastas para exportação. É conveniente criar uma pasta em nível de raiz para cada projeto.

Dentro de uma pasta em nível de processo, é possível criar subpastas. No momento da exportação, a pasta que você exportar como pacote de conteúdo não poderá conter recursos não utilizados ou objetos obsoletos. A estrutura de pastas que você definir para um projeto no ambiente de criação é replicada no ambiente de produção durante a importação.

Siga estas etapas:

1. Decida em que nível deseja a pasta.

   Você pode criar uma pasta no nó raiz ou em uma pasta existente.

2. Clique com o botão direito do mouse no nó pai para a pasta e selecione Novo objeto, Pasta.

   O caminho da pasta é exibido no painel principal com um campo de nome. O nome padrão é exibido como Pasta.

3. Clique no campo Nome, exclua o nome padrão da pasta e digite um nome para essa nova pasta.

Como conceder acesso a pastas

Os administradores (membros do grupo PAMAdmins) têm acesso a todas as pastas e ao conteúdo de todas as pastas.

É possível conceder acesso aos usuários que não são administradores das seguintes maneiras:

- Definir a propriedade de pasta (na página 349).

  A pessoa que cria a pasta (ou o objeto de automação) é o primeiro proprietário. Se você (como um administrador) criar todas as pastas, Definir proprietário é a maneira mais fácil de conceder acesso à pasta aos usuários que não são administradores.

- Criar uma diretiva para cada criador de conteúdo (na página 349).

  É possível conceder acesso a pastas específicas aos criadores de conteúdo (membros de PAMUsers ou um grupo personalizado) que não tenham direitos de Administrador de conteúdo.

Definir a propriedade da pasta

Somente um administrador de conteúdo ou o proprietário da pasta pode alterar a propriedade de uma pasta. Por padrão, o criador da pasta é o seu proprietário. O proprietário tem permissões ilimitadas na pasta. Como administrador de conteúdo, você pode criar uma pasta e transferir a sua propriedade para a ID de usuário apropriada. Por exemplo, os criadores de conteúdo podem ter suas próprias pastas, mas a pasta que é usada para exportar uma versão da release como pacote de conteúdo pode ser atribuída a um administrador.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador:ambiente* apropriado.
3. Selecione uma pasta.
4. Clique em Definir proprietário.
5. Digite a ID do usuário a ser definido como proprietário e clique em Pesquisar.

   Observação: os resultados da pesquisa incluem todos os usuários com uma ID de usuário ou nome de usuário que contêm a sequência de caracteres que você digitar.
6. Selecione o usuário na lista exibida.
7. Clique em Salvar e fechar.

Observação: a propriedade de uma pasta concede acesso à pasta, incluindo a capacidade de exportá-la individualmente ou exportá-la como pacote de conteúdo. Com uma diretiva do CA EEM, você tem mais controle sobre as ações que um criador de conteúdo pode executar em uma pasta.

Criar uma diretiva para cada criador de conteúdo

Assim que sua estrutura de pastas estiver em vigor e os criadores de conteúdo tiverem contas de usuário, você pode conceder acesso à pasta a esses criadores. O acesso à pasta especifica a pasta na qual um usuário ou grupo de aplicativos pode criar e controlar objetos de automação. Esse procedimento pressupõe que você está atribuindo uma pasta separada para cada criador de conteúdo e que essas pastas estão diretamente na pasta raiz.

Uma diretiva personalizada com base no objeto permite conceder acesso à pasta para usuários ou grupos especificados. Os direitos de acesso a pastas disponíveis incluem Listar, Ler, Editar, Excluir e Admin. Depois de criar a primeira diretiva, você pode usar essa diretiva como modelo para criar outras.

Siga estas etapas:

1. Navegue até o CA EEM e efetue logon (na página 46).
2. Clique na guia Manage Access Policies.
3. Clique em Nova diretiva de acesso para Objeto.

   A Nova diretiva de acesso é exibida, na qual o Nome da classe de recurso é Objeto.
4. Digite um nome para essa diretiva que fornece acesso à pasta para um determinado criador de conteúdo.
5. Clique no link Procurar identidades e clique em Pesquisar.
6. Selecione o nome do desenvolvedor de conteúdo e clique na seta para a direita.

   O nome aparece na lista de identidades selecionadas iniciada por [Usuário].
7. Digite o caminho e o nome da pasta criada para este criador de conteúdo no campo Adicionar recurso e clique em Adicionar recurso.
   Sua entrada é exibida na lista de recursos.
8. Selecione cada permissão para conceder ao criador de conteúdo. Por exemplo, conceder todas as ações, exceto Object_Admin.
9. Clique em Salvar.

   A diretiva salva é semelhante ao seguinte:

Nome/Descrição	Nome da classe do recurso	Opções	Identidades	Ações	Recursos
Folder Access for Content Designer 1 Grants Content Designer 1 access to the /ContentDesigner1 folder	Object	Concessão explícita	content designer 1	Object_List Object_Read Object_Edit Object_Delete	/ContentDesigner1

10. Teste o acesso.
    a. Efetue logon no CA Process Automation com as credenciais desse usuário.
    b. Verifique se a única pasta que você pode usar é a que você concedeu acesso.
11. Crie uma diretiva para cada criador de conteúdo adicional de uma das seguintes maneiras:
    - Repita as etapas de 2 a 10.
    - Abra a diretiva salva, clique em Salvar como, digite um novo nome e edite.

Observação: para conceder acesso de leitura para todas as pastas, crie uma diretiva com o objeto para o qual você adicionou todos os criadores de conteúdo. Selecione Object_List e Object_Read para a pasta raiz.

Como gerenciar pastas

Para gerenciar pastas, usar qualquer combinação dos seguintes procedimentos:

- Fazer backup de todas as pastas e do conteúdo correspondente (na página 356).
- Excluir uma pasta (na página 357).
- Exportar uma pasta (na página 353).
- Importar uma pasta (na página 354).
- Mover uma pasta (na página 352).
- Pesquisar na estrutura de pastas (na página 351).
- Mostrar o conteúdo de uma pasta (na página 352).

Observações:

- Consulte o tópico Como preparar o ambiente de produção para uma nova release (na página 358) para obter detalhes sobre a exportação de uma pasta como pacote de conteúdo.
- Consulte o tópico Usar a lixeira (na página 373) para obter detalhes sobre como limpar e restaurar pastas excluídas.

Pesquisar na estrutura de pastas

É possível consultar as pastas com um nome que começa com a sequência de caracteres completa ou parcial que você especificar. O campo de pesquisa fica na parte superior do painel esquerdo da Biblioteca.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador: ambiente* apropriado.
3. Digite o nome completo ou parcial de uma pasta ou de um conjunto de pastas no campo de pesquisa.
4. Examine a lista filtrada. Observe que a pasta no final de cada caminho na lista exibida corresponde aos seus critérios de pesquisa.

Mostrar o conteúdo de uma pasta

Selecione uma pasta para exibir seu conteúdo.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador: ambiente* apropriado.
3. Navegue pela árvore de pastas, expandindo as pastas, conforme necessário. Ou, digite os critérios de pesquisa no campo de pesquisa para filtrar a lista de exibição para pastas que começam com o nome digitado.
4. Quando a pasta de destino for exibida, selecione-a.

   O conteúdo da pasta é exibido no formato de tabela no painel principal.
5. (Opcional) Exibe os dados na ordem desejada. Clique no cabeçalho da coluna que deseja classificar e selecione Crescente ou Decrescente.

Mover uma pasta

É possível mover pastas em uma biblioteca do orquestrador.

Observação: para mover uma pasta de uma biblioteca de orquestrador para outra, exporte a pasta (na página 353).

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador:ambiente* com a biblioteca que contém a pasta de origem.
3. Percorra a árvore de pastas, expandindo as pastas, conforme necessário.

   Observação: digite o nome parcial da pasta para exibir pastas com nomes que começam com a sequencia de caracteres digitada.
4. Quando a pasta de destino for exibida, selecione-a e clique em Recortar.
5. Vá até a pasta de destino e clique em Colar.

   Um dos seguintes resultados é gerado:

   - Se o nome da pasta de destino for diferente do nome da pasta de origem, o orquestrador adicionará a pasta de origem como uma subpasta da pasta de destino.
   - Se as pastas de destino e de origem tiverem o mesmo nome, o orquestrador adicionará o conteúdo da pasta de origem na pasta de destino. Isto é, o orquestrador mescla o conteúdo das duas pastas.

Exportar uma pasta

Ao exportar um dos itens a seguir, o produto cria um arquivo XML que pode ser importado:

- Um objeto.
- Uma pasta que contém vários objetos que são necessários no orquestrador de destino. Os objetos podem não ser relacionados entre si, talvez para processos diferentes. O valor da Versão da release não é aplicável.
- Uma pasta que contém todos os objetos que compõem uma versão da release de um processo. Antes de exportar, você pode define uma Versão da release para a pasta e cada objeto da pasta.

  Observação: para obter mais informações, consulte o tópico Cenário: preparar uma pasta para exportação como pacote de conteúdo.

Os administradores e criadores de conteúdo podem exportar uma pasta do Navegador da biblioteca para um arquivo de exportação no host local. O arquivo de exportação preserva o caminho para a pasta e a estrutura hierárquica dos objetos e pastas secundárias.

Os administradores podem exportar uma pasta das seguintes maneiras:

Exportar, {Caminhos absolutos | Caminhos relativos}

A exportação modificável permite que os destinatários no ambiente de destino atualizem as versões do objetos exportado na pasta.

Exportar como pacote de conteúdo {Caminhos absolutos | Caminhos relativos}

A exportação não modificável não permite que os destinatários no ambiente de destino atualizem as versões do objeto exportado ou o rótulo Versão da release.

Observação: não é possível exportar os objetos que estiverem em várias pastas, como atalhos de um pacote. Em vez disso, crie uma pasta de exportação e, em seguida, agrupe todos os objetos para exportação nessa pasta. Para obter mais informações, consulte o *Guia do Criador de Conteúdo*.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e, em seguida, selecione o *Orquestrador:ambiente* apropriado.
3. Vá para a pasta a ser exportada, clique com o botão direito do mouse na pasta e selecione uma das seguintes opções:
   - Exportar, Caminhos absolutos
   - Exportar, Caminhos relativos

4. Para salvar o arquivo XML, clique em Salvar na caixa de diálogo Download de arquivo.

   Observação: nome de arquivo padrão é *nome-da-pasta*.xml.

5. Na sua unidade local, vá até o local em que deseja salvar o arquivo XML.

6. Defina o nome com o qual deseja salvar o arquivo.

   Por exemplo, anexe _RP ao nome do arquivo para indicar um caminho relativo ou _AP para indicar um caminho absoluto.

   `folder-name_RP.xml`

   `folder-name_AP.xml`

7. Clique em Salvar.

   O produto exporta a pasta e seu conteúdo.

Importar uma pasta

Os administradores de conteúdo podem importar o arquivo XML que representa uma pasta exportada e os objetos contidos nela. Se a pasta tiver sido exportada com o caminho absoluto, a estrutura hierárquica dos objetos e pastas secundárias será preservada no arquivo de exportação. Se a pasta tiver sido exportada com o caminho relativo, a estrutura da pasta de exportação será criada na pasta de importação.

O processo de importação é o mesmo, independentemente de como o conteúdo é exportado. As opções aplicáveis têm como base o conteúdo contido no arquivo de exportação.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador*:*ambiente* de destino.
3. Vá até a pasta de destino da importação.
4. Clique com o botão direito do mouse na pasta e selecione Importar.
5. Execute as seguintes ações na caixa de diálogo Importar:
   a. Clique em Procurar e vá até o local na unidade onde salvou o arquivo exportado.
   b. Selecione o arquivo XML exportado e clique em Abrir.

c. Selecione como importar um objeto que tem o mesmo nome que um objeto existente no mesmo caminho, com base em seu conhecimento sobre os objetos existentes na pasta de importação.

   Importar

   Trate as versões importadas do objeto como uma nova versão do objeto existente. Selecione essa opção se a finalidade desta importação for uma atualização e você desejar manter o histórico de versões anteriores. Se o objeto importado tiver a mesma versão da release, a existente será substituída pela versão da release do objeto importado.

   Substitui a versão da release do objeto importado se um objeto semelhante existir com a mesma versão da release.

   Não importar

   Interrompa a importação do objeto e mantenha o objeto existente. Se você selecionar essa opção, o processo de importação listará os objetos com nomes conflitantes. Se houver conflitos, você poderá importar novamente em uma pasta vazia. Como opção, é possível renomear o objeto no ambiente de origem e, em seguida, repetir a exportação e a importação. Essa opção é ótima quando os objetos que estão sendo importados são objetos novos em vez de novas versões de objetos existentes.

   Importar e substituir

   Exclua o objeto existente e importe uma nova versão do objeto como versão 0.

d. Selecione se deseja definir a versão dos objetos na pasta de importação como atual. A versão atual do processo é a versão executada quando o processo é iniciado. Essa versão se torna ativa após a importação. Outros processos também podem usar os objetos utilizados por esse processo. Se as versões importadas já estiverem definidas como atuais, elas serão imediatamente disponibilizadas para uso. Para obter mais informações, consulte o tópico Determinando se a importação deve ser como atual (na página 366).

e. Selecione se deseja disponibilizar os operadores personalizados.

f. Selecione se deseja publicar o grupo de operadores personalizados na guia Módulos do domínio.

   Observação: não publique um grupo de operadores personalizados, a menos que a pasta que você estiver importando seja de um domínio diferente.

6. Clique em Enviar para iniciar o processo de importação.

7. Clique em OK na mensagem de verificação de importação com êxito.
8. Verifique a pasta importada, bem como seu conteúdo, na pasta atualmente em exibição. Observe os seguintes resultados:
   - Se você exportar a pasta como pacote de conteúdo:
     - Não é possível modificar o valor do atributo Versão da release para nenhum objeto ou para o pacote de conteúdo.
     - Não é possível modificar a versão importada de nenhum objeto. A versão base dos objetos é definida durante a importação.
   - Se você optou por tornar disponíveis os operadores personalizados durante a importação, os operadores personalizados importados estarão disponíveis para uso.
   - Se você publicar o grupo de operadores personalizados na guia Módulos, configure valores para o grupo de operadores personalizados (na página 302).

Fazer backup de todas as pastas e do conteúdo correspondente

É possível fazer backup de uma biblioteca de pastas e de seu conteúdo para se proteger contra perda. Chame uma exportação no nível raiz da estrutura de pastas. O processo de exportação cria um arquivo XML com todas as informações necessárias para recriar as pastas da biblioteca e seu conteúdo após a importação. A melhor prática de segurança é armazenar esse arquivo XML fora do local. Se você perder a biblioteca, será possível reconstruí-la, importando o arquivo XML para o diretório raiz de um novo orquestrador.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador:ambiente* apropriado.
3. Clique com o botão direito do mouse na pasta raiz e selecione Exportar.
4. Determine se deve incluir o caminho completo para os objetos exportados ou o caminho relativo para uma pasta que contém o objeto.
5. Clique em Exportar e selecione um dos seguintes tipos de caminhos:
   - Caminhos absolutos.
   - Caminhos relativos.

   Nos hosts do Windows, a caixa de diálogo Download de arquivo é aberta. Você pode escolher se deseja abrir ou salvar o arquivo.
6. Selecione Salvar.

   Nos hosts do Windows, a caixa de diálogo Salvar como é aberta.
7. Especifique o nome do arquivo com o qual deseja salvar o arquivo XML e o caminho. Por exemplo, librarybackup_*date*.xml
8. Clique em Salvar.

Excluir uma pasta

Você pode excluir as pastas que não forem mais necessárias.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador: ambiente* apropriado.
3. Proceda de uma das seguintes maneiras:
   - Clique com o botão direito do mouse na pasta e selecione Excluir.
   - Selecione a pasta e clique no botão Excluir da barra de ferramentas.

   Uma mensagem de confirmação da exclusão é exibida.
4. Clique em Sim.

   A pasta é excluída.

   Observação: a Lixeira contém objetos de automação excluídos e pastas excluídas. Quando um objeto de automação é restaurado, as pastas excluídas no caminho da pasta original também são restauradas.

Como gerenciar objetos de automação

Os administradores usam a biblioteca para gerenciar os objetos de automação em uma estrutura de pastas. As tarefas de manutenção são as seguintes:

- Definir um novo proprietário para os objetos de automação (na página 358).
- Adicionar tags para uso em pesquisas de objeto.
- Gerenciar versões do objeto.
- Excluir objetos de automação de uma estrutura de pastas.
- Mover um objeto para outra pasta.
- Copiar um ou mais objetos para um orquestrador no mesmo ambiente.

  Consulte Exportar um único objeto e Importar um único objeto.

  Consulte Exportar uma pasta (na página 353) e Importar uma pasta (na página 354).
- Copiar objetos para outro ambiente, por exemplo, de um ambiente de criação para um ambiente de produção.

  Consulte os tópicos Exportar uma pasta como pacote de conteúdo (na página 364) e Importar um pacote de conteúdo (na página 368).

Definir um novo proprietário para os objetos de automação

Somente um administrador de conteúdo ou o proprietário de um objeto de automação pode alterar a propriedade de um objeto de automação. Por padrão, o proprietário de um objeto de automação é a ID de usuário de logon da pessoa que cria o objeto. O proprietário de um objeto tem permissões ilimitadas nesse objeto. Como proprietário de um objeto de automação ou administrador de conteúdo, é possível transferir a propriedade para outro usuário do CA Process Automation. Você também pode definir um novo proprietário para vários objetos de sua propriedade.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador: ambiente* apropriado.
3. Selecione a pasta que contém os objetos de automação de destino.
4. Selecione uma ou mais linhas na grade para os objetos de destino.
5. Clique em Definir proprietário.
6. Especifique a ID de usuário do CA Process Automation do novo proprietário.

Como preparar o ambiente de produção para uma nova release

Os criadores de conteúdo preparam uma pasta para exportação como pacote de conteúdo.

Os administradores de conteúdo verificam se os touchpoints definidos como destinos para os operadores são mapeados para o orquestrador ou agentes no ambiente de produção. Se os administradores de conteúdo concluírem a verificação antes de importar, os objetos poderão ser importados como atuais. Se eles não concluírem a verificação antes da importação, os objetos não serão importados como atuais.

O usuário que realiza a exportação e importação verifica se o processo funciona como previsto no ambiente de produção. Em seguida, os usuários de produção podem começar a usar a nova versão.

A transição consiste nas seguintes etapas:

1. Exportar e importar objetos em um pacote de conteúdo (na página 360).
2. Configurar destinos de produção para o novo processo.
3. Verificar se o processo funciona adequadamente (na página 372).
4. Entregar o novo processo para os usuários de produção.

   Observação: a entrega ocorre fora do aplicativo CA Process Automation.

Sobre a exportação e a importação de um pacote de conteúdo

Um pacote de conteúdo é criado a partir de uma pasta que contém os objetos de automação para uma release específica. Normalmente, a pasta contém os seguintes objetos:

- Um processo, da primeira release ou de uma release posterior.
- Todos os objetos que o processo utiliza.
- Todos os objetos necessários para que os usuários executem o processo.

Antes da exportação, você deve adicionar um valor exclusivo da versão da release à pasta e a cada objeto e verificar se cada objeto tem uma versão base definida. A versão base fornece no ambiente de criação uma versão estática de cada objeto, da forma como ele existia para essa release.

Ao exportar uma pasta como pacote de conteúdo, o CA Process Automation define automaticamente a versão base de todos os objetos no pacote de conteúdo na importação. Pacotes de conteúdo e os objetos contidos neles não podem ser modificados no novo ambiente. (Para tornar um objeto modificável no ambiente de importação, você deve salvar a versão base como uma nova versão.)

Exemplo de versões de release

A guia Release a seguir de uma pasta mostra uma propriedade ReleaseVersion. No exemplo, o Valor é 1.2.3.

O exemplo a seguir é da guia Versões de um processo, onde o valor de Versão da release adicionado corresponde ao valor adicionado para a pasta.

☑		Nome	Tipo	Proprietário
☑		Test1	Processo	pamadmin

Página 1 de 1 | 50 Linhas em cada página | Não há dados para exib

Propriedades

Geral | Tags | Diretiva de arquivamento | ROI | Duração | Segurança em tempo de execução | Versões | Trilha de auditoria

	Versão	Versão da release	Atual	Versão base	Última modificação em
⊞	0	1.2.3	Atual	Versão base	17/09/2013 10:34:39

Observe que uma versão base da Versão da release não foi definida; o botão Versão base está ativado. Quando você observar um objeto destinado para liberação que não possui uma versão base no ambiente de origem, defina a versão que será liberada como uma versão base.

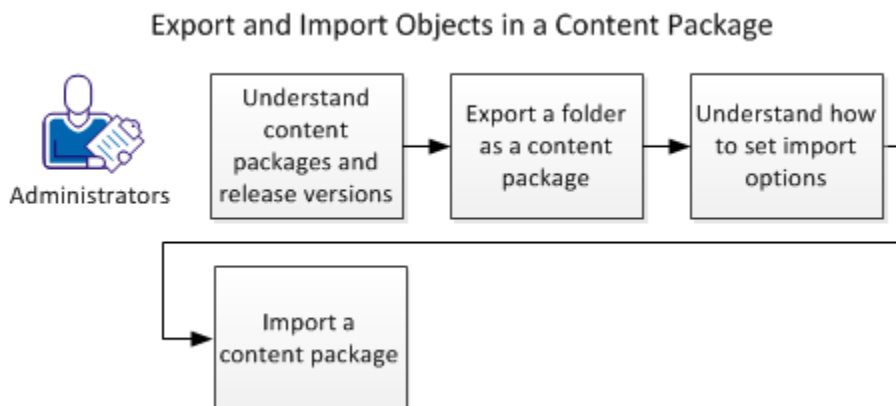
Observação: é possível exportar vários processos de uma vez em uma pasta como pacote de conteúdo e usar o atributo Versão da release para descrever o conteúdo da pasta.

Cenário: exportar e importar objetos em um pacote de conteúdo

Use um pacote de conteúdo para exportar e importar um conjunto de objetos relacionados que compõem uma versão da release de um orquestrador para outro orquestrador. Na maioria dos casos, os orquestradores de origem e de destino estão em ambientes diferentes. Ao exportar uma pasta como pacote de conteúdo, o processo de exportação cria um arquivo XML em sua unidade local. Ao importar para outro orquestrador, você seleciona esse arquivo XML na unidade local. O resultado da importação é o pacote de conteúdo.

Export and Import Objects in a Content Package

Administrators

Understand content packages and release versions → Export a folder as a content package → Understand how to set import options → Import a content package

Siga estas etapas:

1. Entenda a finalidade dos pacotes de conteúdo e das versões de release. Consulte os seguintes tópicos:
   - Sobre os pacotes de conteúdo (na página 361)
   - Sobre as versões de release (na página 363)
2. Exportar uma pasta como pacote de conteúdo (na página 364).
3. Entenda o impacto de definir diferentes opções de importação. Consulte os seguintes tópicos:
   - Determinando se a importação deve ser definida como atual (na página 366)
   - Como definir opções de importação (na página 366)
4. Importar um pacote de conteúdo (na página 368).

Mais informações:

Exemplo: Exportar e importar um pacote de conteúdo (na página 370)

Sobre os pacotes de conteúdo

Os objetos podem ser exportados nos seguintes formatos:

- Um único objeto
- Uma pasta
- Uma pasta como pacote de conteúdo

A exportação de uma pasta como pacote de conteúdo é diferente da exportação de uma pasta das seguintes maneiras:

- O valor de versão da release de qualquer objeto exportado em uma *pasta como pacote de conteúdo* não pode ser modificado após a importação. (Os objetos exportados em uma *pasta* não têm um valor de versão da release.)
- O valor de versão da release de um objeto exportado em uma pasta como pacote de conteúdo não pode ser modificado após a importação.

Exporte uma pasta quando não houver necessidade de atribuir uma versão da release para seus objetos. Por exemplo, exporte objetos de um orquestrador de criação para outro orquestrador de criação em uma pasta.

Exporte uma pasta como pacote de conteúdo ao exportar objetos de um ambiente de criação para um ambiente de produção. Geralmente, os objetos incluídos em um pacote de conteúdo representam uma release de um processo automatizado. Nesse caso, há necessidade de manter a versão de cada objeto, como ele existia no momento da liberação. O pacote de conteúdo inclui:

- A versão da release do objeto de processo.
- Todos os objetos que o processo utiliza.
- Todos os objetos que os usuários de produção usam para iniciar ou interagir com o processo.

Um pacote é uma unidade independente. Um pacote de conteúdo contém uma pasta de objetos que são agrupados para exportação. Antes da exportação, a versão de cada objeto que está sendo exportado é marcada com um valor de Versão da release. O mesmo valor é atribuído como a Versão da release da pasta.

O processo de importação implanta todos os objetos do pacote de conteúdo na biblioteca. Quando importado como atual, o objeto fica disponível para uso. Os usuários no ambiente de importação não podem criar ou alterar os valores de Versão da release.

O processo de importação de pacote de conteúdo define a versão base de cada objeto. A intenção é que a versão da release dos objetos seja usada como está. No entanto, é possível salvar um objeto importado como uma nova versão, alterar o objeto e salvar o objeto alterado como a versão atual. Nesse caso, a versão base definida com o valor de Versão da release permanece intacta. Isso impede que os objetos sejam alterados de forma potencialmente perigosa. Para reverter quaisquer alterações indesejadas, faça com que a versão base definida se torne a versão atual. Os criadores de conteúdo que trabalham com a solução de problemas podem identificar as versões não modificáveis do objeto que foram importadas para o ambiente de produção.

Se você importar um objeto de um provedor de terceiros em um ambiente de criação que deseja alterar, faça uma cópia desse objeto. Em seguida, é possível atualizar a cópia do objeto e atribuir uma versão da release diferente.

Sobre as versões de release

Antes de exportar uma pasta como pacote de conteúdo que contém um processo e seus objetos componentes, o criador de conteúdo executa as seguintes ações:

- Define a versão da release de cada objeto
- Define a versão da release da pasta que contém o(s) objeto(s)

Após a importação, os objetos possuem os mesmos valores de versão da release que você exportou. Ao exportar uma pasta como pacote de conteúdo, o pacote de conteúdo importado está no modo não modificável. Os usuários de destino não poderão modificar o valor de Versão da release que você definir para essa release. O valor de Versão da release ajuda os criadores de conteúdo que trabalham no ambiente de criação a identificar uma versão específica de um objeto no ambiente de produção.

Observação: o CA Process Automation define o bloqueio do atributo Versão da release tanto no objeto quanto na versão da release do objeto. Portanto, os usuários não podem modificar o valor de versão da release do objeto importado, nem definir valores de versão da release para novas versões do objeto.

Os usuários não podem alterar os valores de versão da release não modificáveis após a importação. Considere a necessidade de versões de release de acordo com o que você estiver fazendo com os objetos. Por exemplo:

- Se exportar de um ambiente de *criação* para outro, (opcionalmente) defina os valores do atributo Versão da release e exporte a pasta.
- Se exportar de um ambiente de criação para um *ambiente de produção*, os criadores de conteúdo devem definir os valores do atributo Versão da release para cada objeto e a pasta na qual estão contidos. Em seguida, os criadores exportam essa pasta como pacote de conteúdo.

As seguintes regras controlam a exportação e importação de versões de release:

- Se uma das seguintes instruções for verdadeira, as versões de release serão não modificáveis na importação:
  - Os objetos estão contidos em um pacote de conteúdo.
  - A Versão da release do objeto era não modificável antes da exportação.
- O CA Process Automation define a versão base de versões importadas quando os objetos são importados como pacote de conteúdo (com versões de release não modificáveis).

  Observação: se um objeto for importado novamente com a mesma versão da release, o objeto será substituído.

As seguintes regras controlam a ação de copiar e colar objetos importados:

- A primeira versão da cópia do objeto mantém o valor de Versão da release e o fato de ele ser modificável ou não.
- Se a versão atual do objeto original for definida como base e o atributo Versão da release do objeto for não modificável, a cópia do objeto também será definida como versão base.

Exportar uma pasta como pacote de conteúdo

Os criadores de conteúdo preparam objetos associados com a mesma versão da release para exportação. Em seguida, um criador de conteúdo ou um administrador exporta o pacote de conteúdo. O seguinte procedimento aborda as etapas de preparação e exportação.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador*:*ambiente* de origem.
3. Vá até a pasta de destino. Verifique se a pasta contém todos os objetos que deseja exportar. Verifique se a pasta contém apenas os objetos que deseja exportar.
4. Adicione a versão da release à pasta de destino:
   a. No painel de navegação, selecione a pasta que contém a pasta que deseja exportar.
   b. No painel principal, clique com o botão direito do mouse na pasta que deseja exportar e selecione Propriedades.
   c. Clique na guia Release.
   d. Clique duas vezes na coluna Valor na linha ReleaseVersion.
   e. Digite a versão da release na caixa de diálogo Valor e clique em OK.
   f. Clique em Salvar.

5. Adicione a versão da release à versão selecionada de cada objeto na pasta de destino e certifique-se de que a versão selecionada tem uma versão base definida.
    a. Selecione a pasta de destino que contém os objetos para exportação.
    b. Clique com o botão direito do mouse no objeto e selecione Propriedades.
    c. Selecione a guia Release.
    d. Clique com o botão direito do mouse na linha da versão a ser exportada, selecione Definir a versão da release e digite o mesmo valor de versão da release que você atribuiu à pasta e clique em OK.
    e. Se o valor de Versão base da linha selecionada for Não, clique na guia Versões e clique em Versão base. Clique em Sim para confirmar a definição como versão base.

       Observação: é importante definir a versão base de objetos antes da exportação, para que você sempre tenha uma imagem salva no ambiente de criação de cada objeto no momento do lançamento. (A versão base de todos os objetos é automaticamente definida durante o processo de importação).
    f. Clique em OK.
    g. Repita essas etapas para cada objeto da pasta.
6. No painel de navegação, clique com o botão direito do mouse na pasta e, em seguida, selecione uma das seguintes opções:
    - Exportar como pacote de conteúdo, Caminhos absolutos

      Inclui o caminho completo da pasta selecionada.
    - Exportar como pacote de conteúdo, Caminhos relativos

      Inclui o caminho relativo para a pasta que contém a pasta selecionada.
7. Salve o arquivo do pacote exportado.
    a. Clique em Salvar para salvar o arquivo XML.
    b. Vá até uma pasta em sua unidade local e clique em Salvar.
    c. Quando a caixa de diálogo de download concluído for exibida, clique em Fechar.

   O CA Process Automation exporta o pacote de conteúdo como um arquivo XML. O pacote de conteúdo está pronto para ser importado para outro orquestrador. O arquivo *nome-da-pasta*.xml é criptografado.

Determinando se a importação deve ser definida como atual

Durante uma importação, você deve especificar se deseja importar os objetos como atuais. Importe objetos como atuais quando estas duas instruções forem verdadeiras:

- Todos os destinos são definidos como um touchpoint, um touchpoint do proxy ou um grupo de touchpoints.
- Você configurou destinos de produção para o novo processo.

Observação: é possível importar um processo como atual quando os destinos forem expressões que apontam para variáveis em um conjunto de dados. Ao importar, você pode modificar as variáveis do conjunto de dados para referenciar touchpoints de produção.

O CA Process Automation exige que você aguarde até depois da importação para mapear destinos do operador para hosts de produção apenas se você tiver definido um destino como uma ID de agente, um endereço IP ou um nome do host. Nesse caso, não importe objetos como atuais. Em vez disso, atualize os destinos nos operadores após a importação e marque a versão importada como atual.

Como definir opções de importação

O CA Process Automation fornece certa flexibilidade para importar objetos.

Se um objeto importado tiver o mesmo nome que um objeto existente:
Importar
Importar
Não importar
Importar e substituir

Definir a versão importada como atual
Tornar os operadores personalizados disponíveis
Publicar a configuração do grupo do operador personalizado

Se a importação incluir operadores personalizados, selecione Tornar os operadores personalizados disponíveis.

Se os operadores personalizados forem novos e pertencerem a um novo grupo personalizado, execute a ação apropriada para o seu ambiente.

- Não selecione Publicar a configuração do grupo do operador personalizado se o ambiente de importação estiver no mesmo domínio do ambiente de exportação. Nesse caso, a configuração do grupo de operadores personalizados já foi publicada.
- Selecione Publicar a configuração do grupo do operador personalizado se o ambiente de importação estiver em um domínio diferente do ambiente de exportação

Considere o conteúdo de importação quando você configurar Definir a versão importada como atual e selecionar como lidar com nomes duplicados.

- Para ativar os objetos importados, com a possibilidade de reverter para uma versão anterior de um objeto importado, se necessário:
  - Selecione: Importar
  - Selecione: Definir a versão importada como atual.

  Observação: essas opções são melhores quando você estiver importando uma versão da release de atualização e todos os destinos do operador estiverem configurados como hosts no ambiente de importação. Você pode esperar ser notificado sobre nomes duplicados porque os objetos da última release estão localizados na pasta de destino.

- Para importar sem ativar os objetos atualizados, onde a versão anterior mantém seu status da versão atual:
  - Selecione: Importar
  - Desmarque: Definir a versão importada como atual

  Observação: essas opções são melhores quando a importação incluir operadores que usam hosts de destino que ainda não estão definidos com seu nome de touchpoint no ambiente de importação. Com essa configuração, é possível tornar os objetos atuais depois de verificar se os destinos de processo estão disponíveis no ambiente de importação.

- Para adiar a importação de qualquer objeto com um nome duplicado e optar por tornar os objetos atuais manualmente:
  - Selecione: Não importar
  - Desmarque: Definir a versão importada como atual
  - **Observação:** essas opções são melhores quando você estiver importando novos objetos para uma pasta preenchida. Essas opções evitam que um objeto de importação se torne uma nova versão de um objeto com o mesmo nome, mas com uma função diferente. Essas opções também permitem tornar os objetos atuais depois de testar e verificar o respectivo uso no novo ambiente.

    Se você receber alertas, considere estas ações:

    - Registre os nomes duplicados na mensagem de alerta e informe um administrador no ambiente de origem. Talvez esses objetos possam ser renomeados e exportados novamente.
    - Importe novamente, mas importe para uma pasta vazia.

- Para ativar os objetos importados sem a possibilidade de reverter a ação para os objetos com nomes duplicados:
  - Selecione: Importar e substituir
  - Selecione: Definir a versão importada como atual.
  - **Observação:** essas opções são melhores quando você estiver importando novamente correções de objetos para a pasta de destino. Nesse caso, você nunca precisará reverter para a versão substituída.

Importar um pacote de conteúdo

Os administradores selecionam o orquestrador, selecionam a pasta de destino e, em seguida, chamam a importação. Se o resultado da importação for um pacote de conteúdo, conterá um conjunto de objetos com versão base definida para a mesma release. Você não pode modificar os valores da versão da release de objetos em um pacote de conteúdo importado.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador:ambiente* de destino.
3. Clique com o botão direito do mouse na pasta de destino e selecione Importar.
4. Clique em Procurar e vá até o local na unidade onde salvou o arquivo exportado. Selecione o arquivo XML exportado e clique em Abrir.
5. Selecione como importar um objeto que possui o mesmo nome de um objeto existente no mesmo caminho.
   - Selecione Importar para importar cada objeto como uma nova versão do objeto existente.

     Esta opção é adequada para uma atualização quando você deseja manter o histórico de versões anteriores.

     Observação: se um objeto existente tiver a mesma versão da release do objeto importado, o objeto importado substituirá a versão duplicada.
   - Selecione Não Importar para interromper a importação do objeto e manter o objeto existente.

     Se você selecionar essa opção, o processo de importação listará os objetos com nomes conflitantes. Se houver conflitos, você poderá importar novamente em uma pasta vazia. Como opção, é possível renomear o objeto no ambiente de origem e, em seguida, repetir a exportação e a importação. Essa opção é ótima quando os objetos que estão sendo importados são objetos novos em vez de novas versões de objetos existentes.
   - Selecione Importar e substituir para excluir o objeto existente e importar uma nova versão do objeto como versão 0.

6. Selecione se deseja definir a versão dos objetos na pasta de importação como atual.
   - Selecione Definir a versão importada como atual para ativar a versão importada imediatamente após a importação. Se o objeto importado for uma atualização, os processos existentes que usavam a versão anterior dos objetos passarão a usar a versão importada. Os objetos importados podem incluir um processo com os destinos do operador configurados no ambiente de importação. Nesse caso, é possível verificar o processo atualizado sem precisar redefinir as versões.
   - Desmarque Definir a versão importada como atual para adiar a definição como atual para um processo manual. Por exemplo, desmarque essa opção se a importação contiver um processo no qual os destinos de seus operadores ainda não estiverem definidos nesse ambiente.
7. Selecione se deseja disponibilizar os operadores personalizados importados.
   - Selecione Tornar os operadores personalizados disponíveis para automatizar a definição como disponível para todos os operadores personalizados importados.
   - Desmarque Tornar os operadores personalizados disponíveis para manter um status indisponível para os operadores personalizados importados e disponibilizá-los manualmente, um por um.
8. Selecione se deseja publicar um grupo de operadores personalizados na guia Módulos.
   - Selecione Publicar a configuração do grupo do operador personalizado se a importação incluir novos operadores personalizados e um novo grupo de operadores personalizados e se você estiver importando para um domínio diferente do domínio de exportação.
   - Desmarque Publicar a configuração do grupo do operador personalizado nos seguintes casos:
     - O ambiente de importação está no mesmo domínio que o ambiente de exportação.
     - Os operadores personalizados importados são novas releases de operadores personalizados existentes. Nesse caso, os grupos de operadores personalizados existem.
     - Você prefere que um administrador publique novas configurações do grupo de operadores personalizados manualmente.
9. Clique em Enviar para iniciar o processo de importação.
10. Clique em OK na mensagem de verificação de importação com êxito.

    O pacote é importado com êxito na pasta selecionada. O pacote também é exibido na paleta Pacotes de conteúdo na guia Operações. Quando você seleciona um pacote de conteúdo na paleta, as propriedades são exibidas. A propriedade exibida é o valor de ReleaseVersion que foi definido para a pasta antes da exportação como pacote de conteúdo.

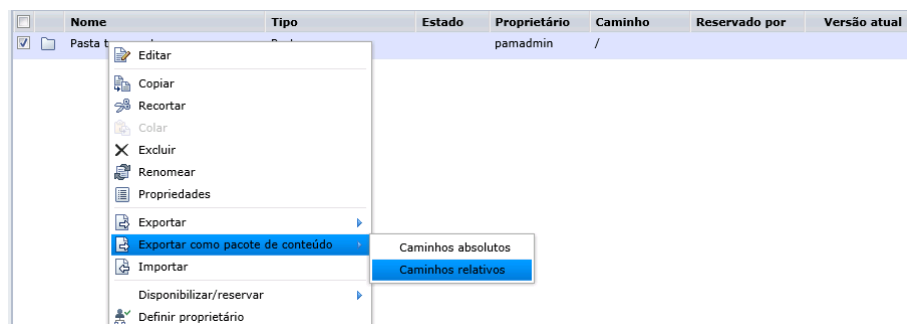
Exemplo: Exportar e importar um pacote de conteúdo

Exporte uma pasta como pacote de conteúdo da biblioteca no ambiente de origem (criação) e salve o arquivo XML resultante. Importe um pacote de conteúdo para a biblioteca do ambiente de destino (produção) procurando o arquivo XML e especificando as opções de importação.

Exportar como pacote de conteúdo

1. Clique na guia Biblioteca do *Orquestrador*:*ambiente* que contém a pasta com os objetos para a transição.
2. Clique com o botão direito do mouse na pasta e, em seguida, selecione Exportar como pacote de conteúdo, Caminhos relativos.

   Essa seleção copia o pacote para uma pasta que não seja a raiz.

Equation 1: As opções de clique com o botão direito do mouse incluem Exportar e Exportar como pacote de conteúdo. Essas duas opções de exportação incluem uma opção de Caminhos absolutos e Caminhos relativos.

3. Salve o arquivo em uma pasta na unidade local ou em uma unidade mapeada.
4. Clique em Abrir pasta. A pasta na qual você salvou o arquivo XML da exportação é exibida quando o download é concluído.

Importar um pacote de conteúdo

1. Clique na guia Biblioteca e selecione o *Orquestrador*:*ambiente* que é o destino do processo de exportação e importação.
2. Vá até a pasta na qual o arquivo XML será importado, clique com o botão direito do mouse na pasta e selecione Importar.

3. Clique em Procurar, vá até o local em que o arquivo foi exportado e clique em Abrir.

   Nesse exemplo, selecione as opções a seguir:

   - Importar
   - Definir versão importada como atual
   - Tornar os operadores personalizados disponíveis

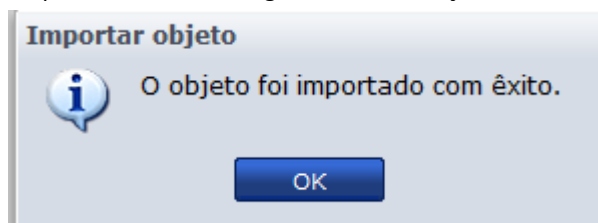
     Observação: se você não selecionar esta opção, o CA Process Automation importará os operadores personalizados como indisponíveis.

     Observação: não selecione Publicar a configuração do grupo do operador personalizado quando o pacote de importação contiver um ou mais operadores personalizados para o qual um novo grupo de operadores personalizados foi publicado para o domínio ao qual o ambiente de importação pertence. O grupo publicado já existirá na guia Módulos no navegador de configuração ao exportar e importar entre ambientes no mesmo domínio.

   Importar
   Arquivo:
   C:\Users\Administrador\Downloads\Pasta to export.xml
   Procurar
   Se um objeto importado tiver o mesmo nome que um objeto existente:
   Importar
   Definir a versão importada como atual
   Tornar os operadores personalizados disponíveis
   Publicar a configuração do grupo do operador personalizado
   Cancelar
   Enviar

4. Clique em Enviar.

5. Clique em OK na mensagem de confirmação.

   Importar objeto
   O objeto foi importado com êxito.
   OK

   O pacote de conteúdo importado é exibido na pasta de importação selecionada. Você também poderá encontrar pacotes de conteúdo na paleta Pacotes de conteúdo na guia Operações. Se você clicar no pacote de conteúdo no painel esquerdo, suas propriedades serão exibidas no painel direito.

6. Na pasta de importação, selecione o pacote de conteúdo importado e clique em Propriedades.
7. Clique na guia Release.

   Os dados de Versão da release do pacote de conteúdo são iguais aos da exportação. Se você apontar para o campo Versão da release, a dica de ferramenta indicará que não é possível modificar o valor de Versão da release.
8. Clique duas vezes no pacote de conteúdo e observe o seguinte:
   - Todos os objetos importados são exibidos na mesma pasta de destino.
   - Todos os objetos importados têm a versão base definida.
   - Todos os objetos importados têm o texto da versão da release que foi definido para o objeto antes da exportação.

Verificar se o processo funciona adequadamente

Antes de ativar o conteúdo de um pacote de conteúdo importado para uso de produção, o administrador executa o processo e monitora os resultados. A execução com êxito indica que a importação do pacote de conteúdo forneceu todos os objetos e componentes necessários e que todos os destinos estão configurados corretamente.

A etapa de verificação pode incluir verificar se o mecanismo de início automático está funcionando, independentemente se for uma programação, formulários, ou disparadores. Ative os disparadores, se necessário.

Em sua forma mais simples, o processo de verificação pode ser resumido conforme descrito a seguir.

Siga estas etapas:

1. Clique na guia Biblioteca e selecione o **Orquestrador**: *ambiente* do destino de importação.
2. Clique na guia Operações.
3. Inicie o processo por meio do mecanismo de início planejado.
4. Monitorar o processo em execução até a conclusão. Responda a todos os formulários para que o processo continue.

5. Caso o processo não seja executado com êxito, retorne-o para o criador de conteúdo para a solução de problemas.
6. Se o processo contiver ramificações, crie os casos para testar as ramificações. Em seguida, inicie o processo e monitore-o.
7. Proceda de uma das seguintes maneiras:
   - Caso o processo não seja executado com êxito, retorne-o para o criador de conteúdo para a solução de problemas.
   - Se o processo for executado com êxito, envie-o para o administrador de produção.
8. Se você identificar qualquer objeto que precise de um trabalho de criação adicional, use o seguinte processo:
   a. Um criador de conteúdo corrige o problema e testa para verificar se ele funciona.
   b. Os criadores de conteúdo preparam uma nova pasta para exportação como pacote de conteúdo. Isso envolve a definição de uma nova versão da release para a pasta e todos os objetos que fazem parte da release. Consulte o tópico Cenário: preparar uma pasta para exportação como pacote de conteúdo.
   c. Exportar e importar novamente essa pasta como pacote de conteúdo. Consulte o tópico Cenário: exportar e importar objetos em um pacote de conteúdo (na página 360).
   d. Verificar novamente se o processo automatizado funciona adequadamente.

Mais informações:

Como preparar o ambiente de produção para uma nova release (na página 358)

Usar a lixeira

A Lixeira contém pastas e objetos que você e outros usuários excluíram da biblioteca.

A ação de *limpar* exclui permanentemente os objetos ou pastas selecionadas da biblioteca.

A ação de *restaurar* restaura os objetos ou pastas selecionadas. A restauração inclui todas as pastas excluídas anteriormente no caminho dos objetos restaurados.

Para obter detalhes, selecione a ação que deseja executar:

- Pesquisar na lixeira (na página 374)
- Restaurar objetos e pastas (na página 375)
- Limpar objetos e pastas (na página 376)

Pesquisar na lixeira

Você pode consultar a lixeira com uma pesquisa básica ou uma pesquisa avançada. A pesquisa básica filtra o nome quando a entrada for o nome inteiro ou uma sequência de caracteres que começa como alguns nomes. A pesquisa avançada contém vários critérios de pesquisa.

Siga estas etapas:

1. Abra o Navegador da biblioteca, reduza a pasta raiz e selecione Lixeira.

   Todos os objetos de automação e pastas atualmente excluídas aparecem na grade principal.

2. Digite uma sequência de caracteres seguida de um asterisco (*) no campo de pesquisa e clique em Pesquisar para executar uma pesquisa básica. Por exemplo, digite Personalizado* para limitar a exibição para os objetos que começam com a sequência de caracteres Personalizado.

   As pastas e os objetos de automação com nomes que correspondem à sua entrada são exibidos na lista filtrada.

3. Clique em Pesquisa avançada para exibir os atributos para pesquisa. Você pode especificar um ou mais tipos de critérios de pesquisa.

   - Palavras-chave - Digite uma ou mais palavras-chave para localizar objetos ou pastas com as palavras-chave especificadas. Se você especificar mais de uma palavra-chave, use a vírgula (,) como delimitador.
     - Para filtrar objetos definidos com qualquer uma das palavras-chave que você especificar, selecione OU, o padrão.
     - Para filtrar objetos definidos com as palavras-chave que você especificar, selecione E.
   - Nome - Nome da pasta ou do objeto de automação.
   - Proprietário - A ID do usuário do proprietário do objeto ou a pasta. O proprietário padrão é o usuário que criou o objeto. Um novo proprietário pode ser especificado em Definir proprietário.
   - Tipo - Selecione um tipo de objeto de automação na lista suspensa.
   - Estado - Selecione um estado na lista suspensa.
   - Data da modificação - Use os calendários para selecionar o intervalo de data durante o qual os itens que você deseja exibir foram modificados.
   - Data de criação - Use os calendários para selecionar o intervalo de data durante o qual os itens que você deseja exibir foram criados.

4. Clique em Pesquisar.

5. Realize a ação de eliminar ou restaurar no conjunto de resultados.

6. Clique em Redefinir para limpar os critérios de pesquisa se você desejar fazer outra pesquisa imediatamente.

Restaurar objetos e pastas

Quando você exclui um objeto ou uma pasta da biblioteca, ele vai para a Lixeira. Da Lixeira, é possível restaurar um objeto ou pasta que você excluiu. Esse processo restaura o objeto ou a pasta e outras pastas no caminho excluído. Você pode especificar se os objetos no caminho de destino que têm o mesmo nome dos objetos selecionados devem ser substituídos.

Siga estas etapas:

1. Clique na guia Biblioteca, reduza a pasta raiz no painel esquerdo e selecione a Lixeira.

   A grade principal é atualizada para exibir todos os objetos e pastas de automação que residem atualmente na Lixeira.

2. Selecione uma ou mais pastas ou objetos e clique em Restaurar o item selecionado.
3. Clique em Sim na mensagem de confirmação para restaurar o item.
   - Se o caminho de destino não contiver nenhum objeto com o mesmo nome de um objeto selecionado, o produto irá restaurar o objeto selecionado no local de destino.
   - Se um objeto no caminho de destino tiver o mesmo nome de um objeto selecionado para uma restauração, será exibido um aviso. Proceda de uma das seguintes maneiras:
     - Selecione o objeto e clique em OK para continuar o processo de restauração.

       O produto move o objeto da Lixeira para o caminho de destino e substitui o objeto existente no caminho de destino.

     - Clique em Cancelar para interromper o processo de restauração do objeto.

       O produto não substitui o objeto no caminho de destino. Nesse caso, considere a possibilidade de mover ou renomear o objeto com o nome duplicado e, em seguida, repetir o processo de restauração.

   O processo restaura os objetos selecionados e, se necessário, o caminho de suas pastas.

Limpar objetos e pastas

A lixeira é criada para ser um recipiente temporário para os objetos excluídos, de modo que os criadores de conteúdo possam restaurar os objetos que sejam excluídos acidentalmente.

A eliminação regular dos objetos obsoletos resulta em uma lixeira organizada. Como administrador, você pode limpar os objetos de automação e pastas que estiverem selecionados. Como alternativa, é possível limpar o conteúdo da lixeira em uma única etapa. Um objeto eliminado não pode ser recuperado ou restaurado.

Siga estas etapas:

1. Clique na guia Biblioteca.
2. Clique em Orquestrador e selecione o *Orquestrador:ambiente* apropriado.
3. Se a lixeira não estiver visível, reduza a pasta raiz.
4. Clique na Lixeira.

   Todos os objetos de automação e pastas que foram excluídos da biblioteca são exibidos no painel principal da grade.
5. Proceda de uma das seguintes maneiras:
   - Selecione os objetos específicos e clique em Limpar os itens selecionados.
   - Clique em Limpar tudo.
6. Se você tiver iniciado a eliminação de objetos selecionados, será exibida uma mensagem de confirmação.
   - Clique em Não para cancelar a eliminação, restaure os objetos necessários na biblioteca e reinicie a eliminação.
   - Clique em Sim para continuar com o processo de eliminação.
7. Se você tiver iniciado um processo de Limpar tudo em que o conteúdo da lixeira inclui objetos reservados, será exibida uma caixa de diálogo que lista esses objetos. Avalie a lista e, em seguida, execute uma das seguintes ações:
   - Clique em Não para cancelar a eliminação, restaure os objetos necessários na biblioteca e reinicie a eliminação.
   - Clique em Sim para continuar com o processo de eliminação.

Apêndice A: Suporte a FIPS 140-2

A publicação 140-2 do FIPS (Federal Information Processing Standard), *Requisitos de segurança para módulos de criptografia*, define um conjunto de requisitos para produtos que criptografam dados confidenciais. O padrão fornece quatro níveis de segurança destinados a cobrir uma grande variedade de possíveis aplicativos e ambientes. A divisão SMA (Security Management and Assurance, gerenciamento e garantia de segurança) do NIST valida os módulos de criptografia e implementações de algoritmo de criptografia. Quando validado, o SMA publica o fornecedor e os números do certificado de validação com nomes de módulos.

Para oferecer suporte ao FIPS 140-2, o CA Process Automation usa os módulos validados criptográficos das bibliotecas RSA BSAFE® Crypto-J. A RSA é a Divisão de Segurança da EMC.

Esta seção contém os seguintes tópicos:

Quando o CA Process Automation usa criptografia

O CA Process Automation criptografa a comunicação e criptografa os armazenamentos de dados. O CA Process Automation usa os módulos validados para FIPS 140-2, conforme necessário, para fins de segurança.

Por exemplo:

- Ao transferir dados entre o orquestrador e os agentes, os dados são criptografados.
- Ao transferir dados do orquestrador ao cliente do CA Process Automation, os dados confidenciais são criptografados.
- Ao transferir dados entre o CA EEM e o CA Process Automation, os dados são criptografados. (Release 03.1.00 e posterior).
- Ao transferir um sistema composto por objetos de automação usando exportar e importar, todos os objetos de senha do sistema são criptografados.
- Quando quaisquer dados confidenciais, como senhas, são armazenados em sistemas de arquivos, esses dados são criptografados.

Módulo de criptografia validado para FIPS 140-2

O CA Process Automation usa um módulo de criptografia incorporado e validado para FIPS 140-2 com estas especificações:

- Certificado nº: 1048
- Fornecedor: RSA, a Divisão de Segurança da EMC
- Módulos de criptografia: módulo de provedor RSA BSAFE® Crypto-J JCE (Versão do software: 4.0)
- Tipo de módulo: software
- Datas de validação: 27/10/2008; 26/01/2009; 07/09/2010
- Nível/Descrição: nível 1 geral
- Algoritmo aprovado pelo FIPS: RSA (cert. #311)

Para obter mais detalhes, use um mecanismo de pesquisa para localizar a *Diretiva de segurança do módulo de provedor RSA BSAFE Crypto-J JCE*. Essa diretiva lista as plataformas em que os algoritmos são compatíveis, incluindo plataformas da Microsoft, Linux, Oracle (Solaris), HP e IBM. Esse documento também inclui detalhes sobre algoritmos do Crypto-J aprovados pelo FIPS.

No modo Apenas FIPS, o CA EEM usa os algoritmos a seguir:

- SHA1, SHA256, SHA384 — Para gerenciar a comunicação cliente-servidor.
- SHA512 — Para armazenar senhas de usuários.

  Observação: o CA EEM aplicará SHA512 ao resumo da senha somente se você atualizar o resumo da senha. Até que você faça a atualização, o CA EEM aceitará a senha existente no resumo.

- SHA256 — Para gerenciar certificados de aplicativo.
- TLS v1.0 — Para a comunicação com diretórios LDAP externos se a conexão LDAP for feita por TLS.

Manter endereços IP

Talvez haja a necessidade de manter endereços IP ou nomes. Os exemplos estão a seguir:

- Altere o endereço IP e o nome de um orquestrador.

  Modifique a combinação de nome e endereço IP sempre que eles aparecerem nos arquivos a seguir.

  install_dir/server/c2o/.config/OasisConfig.properties

  install_dir/server/c2o/.config/Domain.xml

  Observação: para continuar usando o mesmo nome do host em todas as referências do CA Process Automation, modifique o DNS com o novo endereço IP.

- Se você instalar agentes usando endereços IP que se alteram, reconfigure o agente atualizando o seguinte arquivo:

  install_dir/PAM Agent/PAMAgent/.config/OasisConfig.properties

  Altere o valor da seguinte propriedade:

  oasis.jxta.host

- Use vários endereços IP para o CA Process Automation quando tiver dois NICs, um interno e outro externo.

  Para que o CA Process Automation seja associado no endereço IP externo, adicione a seguinte propriedade ao OasisConfig.properties:

  jboss.bind.address=*xxx.xxx.xxx.xxx*

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Autenticação e autorização de usuários no modo FIPS

O CA EEM pode ser configurado para usar o modo FIPS. Isto é uma opção. Somente se o CA EEM estiver configurado para usar o FIPS, o CA Process Automation poderá ser configurado para usar o FIPS. Mesmo se o CA EEM estiver configurado para usar o FIPS, o CA Process Automation poderá ser configurado para não usar o FIPS.

Esteja o modo FIPS definido como ativado ou desativado, os dados transferidos entre o CA EEM e o CA Process Automation serão criptografados. A diferença está nos algoritmos usados para criptografia.

Quando os usuários efetuam logon, o CA Process Automation transfere o nome de usuário e a senha para o CA EEM. O CA EEM retorna os dados de autenticação e autorização para o CA Process Automation.

- Quando o modo FIPS está ativado:
  - Os dados transferidos são criptografados com o algoritmo SHA1 com suporte pelo FIPS.
  - Um certificado PAM.cer é usado.
- Quando o modo FIPS está desativado:
  - Os dados transferidos são criptografados com o algoritmo MD5.
  - Um certificado PAM.p12 é usado.

Apêndice B: Mantendo o domínio

Manter o domínio envolve algumas tarefas que você executa fora da guia Configuração.

Esta seção contém os seguintes tópicos:

Criar o domínio

A criação de um sistema inclui alterações lógicas e físicas. Você pode criar seu sistema físico por meio da instalação. Você pode criar seu sistema lógico no CA Process Automation.

- Se for necessária capacidade adicional no ambiente de criação, adicione um nó ao orquestrador de domínio.
- Se for necessária capacidade adicional no ambiente de produção, adicione um nó ao orquestrador usado para produção. Adicione um balanceador de carga de hardware ou software.

  Observação: consulte o *Guia de Instalação* para obter detalhes.
- Se um servidor no qual um orquestrador está instalado estiver sendo retirado de serviço, exporte o nó raiz da biblioteca e importe-o no novo orquestrador.
- Quando novos usuários forem necessários ou novas funções forem adicionadas, atualize o CA EEM com alterações nas contas de usuário e diretivas.

Fazer backup do domínio

Faça backup do CA Process Automation com a ferramenta de backup que você usa no seu site.

Siga estas etapas:

1. Faça backup de cada ocorrência dos três bancos de dados do CA Process Automation a seguir:
   - Repositório
   - Tempo de execução
   - Geração de relatórios
2. Faça backup da seguinte pasta:

   install_dir/server/c2o/.config
3. Faça backup do conteúdo da biblioteca exportando a pasta raiz na guia Biblioteca.

Restaurar o domínio usando backups

O CA Process Automation pode falhar devido à corrupção de dados, configuração errada, ou perda de armazenamento em um orquestrador de domínio agrupado. É possível se recuperar de uma falha e restaurar os dados para o CA Process Automation.

Você pode restaurar seu uso do CA Process Automation após uma falha. A abordagem é executar uma nova instalação do orquestrador de domínio, que você deve encerrar assim que estiver instalado. Você pode substituir os bancos de dados vazios pelos backups de seus bancos de dados e restaurar seu arquivo de configuração a partir de um backup. Em seguida, você deve iniciar o CA Process Automation e verificar se os dados foram restaurados.

Siga estas etapas:

1. Prepare-se para a instalação. Consulte o *Guia de Instalação* durante a preparação a seguir:
   - Verifique se o hardware, o sistema operacional e o mecanismo de banco de dados estão instalados.
   - Verifique se os componentes de terceiros necessários estão instalados.
   - Instale e configure o CA EEM.
2. Execute uma nova instalação do CA Process Automation, como descrito no *Guia de Instalação*.
3. Adicione os nós conforme necessário para refletir o agrupamento original. Consulte o *Guia de Instalação* para obter detalhes.
4. Interrompa o CA Process Automation.
5. Restaure seu sistema com os backups.
   a. Substitua o banco de dados do repositório, o banco de dados de tempo de execução e o banco de dados de relatórios usando os respectivos backups de banco de dados.
   b. Renomeie a pasta .config atual em:

      install_dir/server/c2o/.config
   c. Restaure o seguinte do backup:

      install_dir/server/c2o/.config
6. Inicie o CA Process Automation.
7. Verifique se sua configuração foi restaurada.
8. Verifique se o banco de dados está intacto.

Gerenciar Certificados

O gerenciamento de certificados envolve os seguintes procedimentos:

- Instalar o certificado predefinido do CA Process Automation (na página 385).
- Criar e implementar seus próprios certificados para o CA Process Automation (na página 387).
- Implementar o certificado SSL confiável de terceiros para o CA Process Automation (na página 390).

Como o CA Process Automation protege as senhas

Credenciais de conta de usuário, nome de usuário e senha são usados para acessar vários sistemas e recursos. O valor da senha devem ser protegidos por razões de segurança. Embora as senhas sejam sequências de caracteres, elas são tratadas de forma diferente de outros valores desse tipo de dados. O CA Process Automation protege as senhas no nível de UI das seguintes maneiras:

- Os usuários não podem transferir senhas de um lugar para outro.
- Os usuários não podem gravar um processo do CA Process Automation que diz process.v = process.Password, pois V está visível.
- Manipulações como anexar uma senha com a letra "t" e, em seguida, mais tarde mover o "t" são desativadas usando JavaScript.
- Os usuários não podem concatenar senhas com um operador +. Nenhuma ação que possa revelar o valor de senha é permitida.
- Os usuários não podem ativar conteúdo com detecção de senha. Por exemplo, eles não podem produzir o que está visivelmente oculto.

Em resumo, o CA Process Automation ajuda a garantir a privacidade, contanto que a senha esteja no CA Process Automation. As senhas que fazem parte das configurações de categoria do operador são protegidas. Elas não podem ser modificadas, referenciadas ou transmitidas para métodos externos.

Quando uma senha que não faz parte de uma configuração de categoria de operador é transmitida para um método externo, ela pode ser retornada em texto não criptografado. Tome medidas para proteger senhas que são passadas para programas externos. A melhor solução é usar certificados ou uma alternativa.

É possível exportar o conteúdo das definições armazenado em um banco de dados e, em seguida, importá-lo para um banco de dados no mesmo domínio ou em um domínio diferente. Importar conjuntos de dados para outro domínio anula as senhas, uma vez que as senhas são criptografadas. Isso é estrutural; domínios diferentes usam diferentes chaves de criptografia.

Sobre o certificado do CA Process Automation

Pesquise as diferenças entre usar um certificado autoassinado e um certificado SSL confiável em relação às suas necessidades de segurança para o CA Process Automation.

O CA Process Automation fornece um certificado autoassinado pré-configurado para uso. É possível gerenciar o certificado do CA Process Automation de qualquer uma das seguintes maneiras:

- Usar o certificado fornecido com o CA Process Automation. Instale esse certificado de cada navegador do qual você acessar o URL para o Orquestrador de domínio do CA Process Automation.
- Crie seu próprio certificado autoassinado com um utilitário fornecido, criptografe a senha com um utilitário fornecido, atualize o arquivo de propriedades com o local do keystore, a senha criptografada e o alias do keystore.
- Obtenha um certificado de uma Autoridade de certificação reconhecida. Atualize o arquivo de propriedades com o local do keystore, a senha criptografada e o alias do keystore.

Importante: Não remova o keystore padrão ou o certificado autoassinado fornecido com o CA Process Automation. Esse certificado é necessário mesmo quando você configura o CA Process Automation para usar seu próprio certificado autoassinado ou o obtido da CA..

Instalar o certificado pré-definido do CA Process Automation

Se você acessar o CA Process Automation com um URL que use o protocolo HTTPS, o navegador verificará se há um certificado emitido por uma Autoridade de certificação (CA). Se você estiver usando o certificado autoassinado da CA Technologies ao iniciar o CA Process Automation, o navegador exibirá um aviso de que o certificado não é confiável.

Para instalar o certificado pré-definido para o CA Process Automation

1. Abra um navegador, digite o URL para o CA Process Automation e efetue logon.
2. Se um Alerta de segurança for exibido, clique em Exibir certificado.
3. Clique em Instalar certificado e clique em OK.
4. Conclua o assistente.

   Na próxima vez que você fizer o logon, nenhum Alerta de segurança será apresentado.

Sobre a criação de um certificado autoassinado

Você pode substituir o certificado autoassinado fornecido com o CA Process Automation. O certificado pré-definido está configurado no arquivo OasisConfig.properties. Quando você criar seu próprio certificado autoassinado, atualize o arquivo de propriedades e execute um arquivo em lote para assinar os arquivos Jar (Java ARchive).

Antes de criar o seu próprio certificado, planeje os valores do caminho e do alias de keystore. Insira esses valores ao executar o keytool e atualizar o arquivo de propriedades.

Você usa os seguintes arquivos e utilitários para implementar seus próprios certificados autoassinados:

- Utilitário keytool

  Observação: para obter detalhes sobre esse utilitário Java Sun, procure keytool - Ferramenta de gerenciamento de chaves e certificados.

- PasswordEncryption.bat
- SignC2OJars.bat
- Arquivo OasisConfig.properties, especificamente, os seguintes três parâmetros
  - itpam.web.keystorepath=

    Padrão:

    install_dir/server/c2o/.config/c2okeystore

    Observação: o padrão é o caminho do armazenamento de chaves autoassinado,

  - itpam.web.keystore.password=

    O padrão aponta para o DomainID criptografado. (Execute o arquivo PasswordEncryption.bat, digite a senha do keystore. O programa em lotes gera a senha criptografada no console, que você especifica aqui como o novo valor).

  - itpam.web.keystorealias=

    Padrão: ITPAM

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Criar e implementar seu próprio certificado autoassinado

É possível criar seu próprio certificado autoassinado para substituir o fornecido com o CA Process Automation.

Siga estas etapas:

1. Usando credenciais de administrador, efetue logon no host em que o orquestrador de destino está instalado.
2. Interrompa o orquestrador (na página 193).
3. Se você pretende reutilizar o nome do alias atual do keystore, remova esse alias antes de continuar.
4. Execute o comando a seguir para gerar um keystore com a ferramenta Java keytool. Especifique seus próprios valores para aliasname e keystore_name. O valor padrão para aliasname é ITPAM. Se você não digitar um caminho para o keystore, o caminho atual será usado.

   ```
   keytool -genkey -alias "aliasname" -keyalg RSA -keystore
   "keystore_path.keystore"
   ```

   Por exemplo, aceite o caminho padrão de armazenamento de chaves e digite:

   ```
   keytool -genkey -alias "PAM" -keyalg RSA
   ```

   Os prompts para digitar e confirmar uma senha do keystore são exibidos.

5. Digite a mesma senha de keystore em resposta aos dois prompts. (Memorize essa senha para inserir mais tarde em um utilitário de criptografia).

   Uma série de prompts é exibida, seguida por um prompt de confirmação.

6. Responda aos prompts com as informações do nome distinto solicitadas, como a seguir:

   a. Digite seu nome e sobrenome.

   b. Digite o nome da unidade organizacional.

   c. Digite o nome da organização.

   d. Digite o nome da sua cidade ou localidade.

   e. Digite o nome do seu estado.

   f. Digite o código de duas letras do país para a unidade organizacional.

   Uma confirmação de suas entradas é exibida no formato: CN=value, OU=value, O=value, L=value, ST=value, C=value correto?

7. Examine o que foi digitado e, se estiver correto, digite Sim. (Se estiver incorreto, digite não e responda novamente aos prompts).

8. Responda ao prompt da senha da chave para *aliasname* de uma das seguintes formas. A opção recomendada permite evitar digitar a senha do certificado à medida que cada jar é assinado na Etapa 13.

   - Digite uma senha da chave exclusiva para *aliasname*.
   - (Recomendado) Pressione Enter para usar a senha do keystore como a senha do alias.

   Um novo keystore é criado no diretório atual.

9. (Opcional) Mova esse keystore para outro caminho.

10. Criptografe a senha do keystore inserida na Etapa 5.

    a. Altere os diretórios para o diretório *install_dir*/server/c2o directory.

    b. Execute o PasswordEncryption.bat.

    c. Digite a senha do keystore em resposta ao prompt.

    O utilitário criptografa a senha do keystore digitada e salva os resultados no console.

11. Faça backup do arquivo OasisConfig.properties. (*install_dir*/server/c2o/.config/OasisConfig.properties)

12. Atualize o arquivo de propriedades OasisConfiguration como segue:

    a. Para itpam.web.keystorepath=, digite o caminho absoluto para o keystore, usando "/" em vez de "\", por exemplo, C:/*keystore_path*/keystore.

    b. Para itpam.web.keystore.password=, copie e cole a senha do keystore criptografada gerada na Etapa 9.

    c. Para itpam.web.keystore.alias=, digite o nome do alias especificado no comando do keytool na Etapa 4.

13. Executar o SignC2OJars.bat para assinar os Jars.

    Esta etapa é necessária após a atualização do certificado ou keystore.

14. Inicie o orquestrador (na página 194).

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Sobre o uso de um certificado emitido por uma Autoridade certificadora de terceiros

O CA Process Automation oferece suporte aos certificados de segurança de terceiros para o acesso HTTPS à web e a assinatura de jars. Use seus próprios recursos para obter um certificado SSL confiável da Autoridade de certificação de sua escolha. Esse procedimento está além do escopo deste guia.

A utilização de certificados de segurança de terceiros requer o uso de ferramentas de terceiros. O processo de instalação também requer alterações manuais no arquivo de propriedades OasisConfig (*install_dir*/server/c2o/.config/OasisConfig.properties). Antes de começar, familiarize-se com os conceitos básicos de certificados de segurança e armazenamentos de chaves, e com o utilitário keytool fornecido com o Java JDK.

A implementação de certificados de segurança de terceiros requer a atualização de valores de três parâmetros no arquivo de propriedades OasisConfig:

- "itpam.web.keystorepath"

  O valor padrão é o caminho de keystore para o certificado autoassinado:

  `install_dir/server/c2o/.config/c2okeystore`

- "itpam.web.keystore.password"

  O valor padrão é o "DOMAINID" criptografado.

- "itpam.web.keystorealias"

  O valor padrão é ITPAM.

  Observação: um keystore pode ter mais de um alias. Para usar um alias de keystore que duplique um alias existente, remova o alias existente antes de adicionar uma nova instância.

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Implementar o certificado SSL confiável de terceiros

O CA Process Automation oferece suporte aos certificados de segurança de terceiros para o acesso HTTPS à web e a assinatura de jars. Você pode obter esses certificados de uma Autoridade certificadora de terceiros.

Siga estas etapas:

1. Decida uma senha para o certificado e obtenha um certificado de segurança de uma Autoridade de certificação.
2. Usando as instruções fornecidas pela Autoridade certificadora, importe o certificado para um armazenamento de chaves.

   Geralmente, você usa um comando similar ao keytool –import –alias *myalias* –file certfile –keystore "path_and_file_specification_for_keystore".
3. Para a senha do keystore, digite a senha do certificado fornecida pela Autoridade de certificação.
4. Obtenha uma versão criptografada da senha do keystore.
   a. Vá para *install_dir*/server/c2o.
   b. Localize o script PasswordEncryption (PasswordEncryption.bat para Windows, PasswordEncryption.sh para UNIX ou Linux).
   c. Execute o PasswordEncryption passwordtoencrypt.
   d. Salve o valor longo criptografado retornado para a entrada no arquivo de propriedades.
5. Interrompa o orquestrador (na página 193).
6. Faça o backup e edite o arquivo de propriedades Oasis Configuration para adicionar ou atualizar o seguinte:
   a. itpam.web.keystorepath para o local do keystore usando o caminho totalmente qualificado e um nome para o arquivo de keystore.
   b. itpam.web.keystore.password com a senha do armazenamento de chaves criptografada (não coloque o valor da senha criptografada entre aspas)
   c. itpam.web.keystorealias para o alias usado para referenciar o certificado no armazenamento (myalias nos exemplos).
7. Assine o jars executando SignC2OJars (SignC2OJars.bat para Windows, SignC2OJars.sh para UNIX ou Linux) incluído no CA Process Automation em <*install_dir*>\server\c2o. Execute SignC2oJars sem parâmetros para assinar os jars. Se a senha do keystore digitada não corresponder à senha do certificado, digite a senha do certificado à medida que cada jar for assinado.

   Observação: no AIX, há um problema conhecido ao assinar novamente um arquivo jar usando o SignC2oJars. Para contornar esse problema, remova a assinatura manualmente, removendo os arquivos *.SF e *.RSA na pasta META-INF para cada arquivo Java antes de executar o SignC2oJars.

8. Se o keystore contiver mais de um alias, modifique a entrada do conector no server.xml. O server.xm. está localizado em <install_dir>\server\c2o\deploy\jbossweb-tomcat55,sar\server.xml. Adicione a linha em negrito:

```
<Connector port="${tomcat.secure.port}"
address="${jboss.bind.address}"
   maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
   emptySessionPath="true"
   scheme="https" secure="true" clientAuth="false"
   keystoreFile="${itpam.web.keystorepath}"
   keyAlias="${itpam.web.keystorealias}"
   keystorePass="${itpam.web.keystore.password}" sslProtocol =
   "${SSL_PROTOCOL}" algorithm = "${X509_ALGORITHM}"
   useBodyEncodingForURI="true"/>
```

9. Inicie o orquestrador (na página 194).
10. Repita esse procedimento para cada Orquestrador que deverá usar o novo certificado.

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Manter o nome de host DNS

É possível modificar o nome de host para um orquestrador. Por exemplo, se o nome de host não estiver de acordo com a sintaxe com suporte, você poderá atualizá-lo. Se você tiver instalado o CA Process Automation usando um nome de host DNS inválido contendo caracteres restritos, como sublinhados, crie um alias que esteja de acordo com os padrões de DNS. Em seguida, substitua manualmente o nome de host inválido por esse alias no arquivo OasisConfig.properties.

Siga estas etapas:

1. Crie um alias. Consulte o tópico Ativar o DNS para resolver um nome de host inválido.
2. Efetue logon como administrador no servidor em que o orquestrador de domínio está instalado.
3. Vá até a seguinte pasta, em que install_dir faz referência ao caminho em que o orquestrador de domínio está instalado:

   `install_dir/server/c2o/.config`
4. Abra o arquivo OasisConfig.properties com um editor.
5. Use Localizar para encontrar a seguinte propriedade:

   `oasis.local.hostname`
6. Altere o valor da propriedade oasis.local.hostname=.
7. Salve o arquivo e saia.
8. Reinicie o serviço do orquestrador.
   a. Interrompa o orquestrador (na página 193).
   b. Inicie o orquestrador (na página 194).

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Sintaxe de nomes de host DNS

Há muitos locais onde você pode digitar um FQDN ou um endereço IP. Se os nomes de host DNS incluírem um caractere sublinhado ou, de qualquer maneira, não estiverem de acordo com a sintaxe exigida, especifique o endereço IP.

Os nomes de host DNS válidos:

- Começam com um caractere alfabético.
- Terminam com um caractere alfanumérico.
- Contém de 2 a 24 caracteres alfanuméricos.
- Podem conter o caractere especial de sinal de subtração (-).

  Importante: o sinal de subtração (-) é o único caractere especial válido permitido em nomes de hosts DNS.

Desativar o Catalyst Process Automation Services

O Catalyst Process Automation Services é ativado por padrão. É possível desativá-lo alterando um valor de propriedade no arquivo OasisConfig.properties.

Siga estas etapas:

1. Efetue logon como administrador no servidor em que o orquestrador de domínio está instalado.
2. Interrompa o orquestrador (na página 193).
3. Vá até a seguinte pasta:

   install_dir/server/c2o/.config
4. Abra o arquivo OasisConfig.properties
5. Role até o conector incorporado UCF na seção jboss-service.xml do arquivo OasisConfig.properties.
6. Altere o valor de ucf.connector.enabled para false. Por exemplo:

   ```
   ucf.connector.enabled=false
   ```
7. Salve o arquivo e saia.
8. Inicie o orquestrador (na página 194).

Mais informações:

Arquivo de propriedades de configuração do Oasis (na página 397)

Apêndice C: Referência OasisConfig.Properties

Esta seção contém o seguinte tópico:

O arquivo de texto OasisConfig.properties controla o CA Process Automation. As seleções feitas pelo instalador ao instalar o Orquestrador de domínio, seus pré-requisitos e seus objetos são armazenadas como valores de parâmetros no arquivo OasisConfig.properties.

Importante: Restrinja a atualização do arquivo OasisConfig.properties a um administrador confiável.

Este guia inclui os seguintes tópicos sobre a atualização do arquivo OasisConfig.properties:

- Caches de controle de atualizações do CA EEM (na página 78).
- Alterar a porta de escuta de SNMP Traps (na página 325).
- Configurar as propriedades do domínio (na página 146).
- Controlar o tempo limite do CA Process Automation (na página 20).
- Criar e implementar seu próprio certificado para o CA Process Automation (na página 387).
- Desativar o Catalyst Process Automation Services (na página 393).
- Implementar o certificado SSL confiável de terceiros para o CA Process Automation (na página 390).
- Manter o nome de host DNS (na página 392).
- Manter endereços IP (na página 379).
- Definir o número máximo de usuários e grupos do CA EEM (na página 63).

O *Guia de Instalação* inclui os seguintes tópicos sobre a atualização do arquivo OasisConfig.properties:

- Ativar logoff no CA Process Automation para SSO
- Ativar a autenticação de passagem NTLM após a instalação
- Gerar arquivos de certificado SSL
- Manter o nome de host DNS
- Pré-requisitos do planejamento de portas
- Resolver o conflito de porta com o agente

A *Referência do criador de conteúdo* inclui o seguinte tópico sobre a atualização do arquivo OasisConfig.properties:

- Portas do operador

A *Referência dos Serviços Web* inclui os seguintes tópicos sobre a atualização do arquivo OasisConfig.properties:

- Comunicações
- executePendingInteraction

Arquivo de propriedades de configuração do Oasis

O arquivo de propriedades de configuração do Oasis (OasisConfig.properties) contém as configurações de propriedade de todos os aspectos do CA Process Automation. O arquivo está localizado na pasta *diretório_de_instalação*/server/c2o/.config. Todos os usuários com acesso ao local de instalação do CA Process Automation podem modificar os arquivos. Considere restringir o acesso a esse local. Alguns valores *não* devem ser editados.

As configurações incluem:

USE_DEPRECATED_COMMS_V1

(Somente para agentes) Durante a inicialização de um agente, determina se ele usa o novo modo de comunicação ou o modo de comunicação obsoleta. Este é um valor booleano.

Quando a caixa de seleção Usar comunicação obsoleta nas propriedades de um agente estiver marcada, esse valor será configurado como true. CA Process Automation:

- Encerra a conexão de soquete da web do agente e, em seguida, passa essas informações para todos os orquestradores antes do término.
- Limpa o mapa do servidor em que esses detalhes da conexão estão armazenados.

Quando a caixa de seleção Usar comunicação obsoleta nas propriedades de um agente não estiver marcada, esse valor será configurado como false.

- O agente criará uma conexão de soquete e enviará os detalhes da conexão para o orquestrador.
- O orquestrador salvará esses detalhes da conexão em um mapa do servidor.

Consulte o tópico Determinar o modo de comunicação do agente (na página 217) para obter mais informações.

DOMAINID

Define a ID exclusiva do domínio.

Exemplo

`ac04f945-f08b-4308-aa9c-c3fd95964f4d`

CLUSTERNODEID

Determina um nó em um cluster de forma exclusiva.

Exemplo

`8d11558a-3bf7-43d9-b394-4c055229e9ae`

KEYSTOREID

Define a senha do armazenamento de chaves.

Exemplo

```
ac04f945-f08b-4308-aa9c-c3fd95964f4d
```

itpam.web.keystorepath

Define o caminho do armazenamento de chaves usado para assinar jars.

Exemplo

```
C:/Arquivos de
Programas/CA/PAMcert_Java7_Node2/server/c2o/.config/c2okeys
tore
```

itpam.web.keystore.password

Define a senha do armazenamento de chaves usado para assinar jars.

Exemplo


```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZLQotQj5
5Y8dPGRRXkrF4yTyk/IwzTcT0rLY+pWeGrGHaRKnlcXHL3fr7pYIzjVhoGd
rnRxSO4Prl70rIxqs3fCGIgFVIAnOzICQ9ct4qXIBIPnxQcgflrF0WDdaIj
CS6ubKwe9Wxhn0xjnmctvkLnMC1L74b48yQd9yhWSMAgpLAPLPJiMz/VoIz
cFVylqLS44KdM+wH6b6xkqVJECSH1GolBG2QUj/2
```


itpam.web.keystorealias

Define o nome do alias do certificado no armazenamento de chaves que é usado para assinar jars.

Exemplo

```
ITPAM
```

CERTPASSWORD

Define a senha usada para controlar o acesso ao armazenamento de chaves usado para criptografar senhas e outros dados críticos.

Exemplo


```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZXNASLuj
iOdl6POYm8CwjBTHnFUlbXQLcPqd+xc7oJkPF5X3cq8UHbEYL4iH+01b1Em
wHhw9uPXqDABcJqIJ+ECmODDAMn7rytSWqli+oxKp+e5scp1fnHjF1ENCKZ
NasYy6nF6vPozT9qLmB7DhzuFAvg8Av9J/U4ngYrZ5AMdU1sFP5Ddf3nw==
```


oasis.database.username

Define o nome de usuário do servidor de banco de dados da biblioteca.

Exemplo

```
sa
```

oasis.database.password

Define a senha associada ao usuário especificado do servidor de banco de dados da biblioteca.

Exemplo

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZSSb28pT
xSL4fxuv+8IV8zLz+S6jwleU4mpQTDTM1xmwQ037qmAjDO74Y569W3LIP0v
BUEkJ30raf3/RsodMLdL3L51cnz8Gus4mJfGJla7WdTtzx0ts0BuUFPxZ1p
OpHOUUljFHn73243Iv7/pXIQe+O8lrHB00XotDicrleXavs+8sXSIPqKyX3
gmjy6LUZ
```

oasis.database.dbhostname

Define o nome do host do servidor de banco de dados da biblioteca.

Exemplo

```
lodivsa205
```

oasis.database.dbport

Define o número da porta de conexão com o servidor de banco de dados da biblioteca.

Exemplo

```
1433
```

oasis.database.connectionurl

Define o URL de conexão JDBC do banco de dados da biblioteca.

Exemplo

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.database.databasetype

Define o tipo de banco de dados da biblioteca.

Exemplo

```
MSSQLServer2005
```

oasis.database.dialect

Define a classe de dialeto do banco de dados da biblioteca, definida pelo usuário.

Exemplo

```
com.optinuity.c2o.persistence.MSQLServerDialect
```

oasis.database.genericdialect

Define a classe de dialeto do banco de dados da biblioteca.

Exemplo

```
org.hibernate.dialect.SQLServerDialect
```

oasis.database.driver

Define o nome totalmente qualificado da classe de driver do JDBC.

Exemplo

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.database.typemapping

Define o mapeamento de tipo da fonte de dados.

Exemplo

```
MS SQLSERVER2000
```

oasis.database.exceptionsorter

Define uma classe que implementa a interface org.jboss.resource.adapter.jdbc.ExceptionSorter. A interface examina exceções do banco de dados para determinar se elas indicam um erro de conexão.

Exemplo

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

oasis.database.validConnectionChecker

Define uma classe que implementa a interface org.jboss.resource.adapter.jdbc.ValidConnectionChecker. A interface fornece um modo SQLException isValidConnection(Connection e). O aplicativo chama o modo com uma conexão que retorna do pool para testar sua validade.

Exemplo

```
org.jboss.jca.adapters.jdbc.extensions.mssql.MSSQLValidConn
ectionChecker
```

oasis.database.datasource.class

Define a classe da fonte de dados.

Exemplo

```
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
```

oasis.database.additionalparamurl

Define parâmetros usados para criar a conexão do banco de dados.

Exemplo

```
responseBuffering=full;SelectMethod=cursor;
```

oasis.database.lib.dbname

Define o nome do banco de dados da biblioteca.

Exemplo

```
pamgacert_cluster_JDK7_rep
```

oasis.database.queues.dbname

Define o nome do banco de dados de filas.

Exemplo

```
pamgacert_cluster_JDK7_run
```

oasis.reporting.database.databasetype

Define o tipo do banco de dados de relatórios.

Exemplo

```
MSSQLServer2005
```

oasis.reporting.database.username

Define o nome de usuário do servidor de banco de dados de relatórios.

Exemplo

```
sa
```

oasis.reporting.database.password

Define a senha associada ao usuário especificado para o servidor de banco de dados de relatórios.

Exemplo

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZoIzz9oH
5OU4XRkOaeLblNqEYDsaXNGiMg9LSy2P7gsVLG0ea32nBlUIvXgEXhiKfGz
IbCmYFgYoFg0sVBlnY/k1sAeZ21z20sw5Yr9HC2B3+IRoyy5LXCmByMUMc7
Ywq/BocPnw4e1DBDDfGqCQL/6ciK4CT1C7hU/V3Y4Ktrc9IsPK1aXeNRM1q
vpVwBAtG
```

oasis.reporting.database.dbhostname

Define o nome do host do servidor de banco de dados de relatórios.

Exemplo

```
lodivsa205
```

oasis.reporting.database.dbport

Define o número da porta de conexão com o servidor de banco de dados de relatórios.

Exemplo

```
1433
```

oasis.reporting.database.genericdialect

Define a classe de dialeto do banco de dados de relatórios.

Exemplo

```
org.hibernate.dialect.SQLServerDialect
```

oasis.reporting.database.driver

Define o nome totalmente qualificado da classe de driver do JDBC.

Exemplo

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.reporting.database.typemapping

Define o mapeamento de tipo da fonte de dados.

Exemplo

```
MS SQLSERVER2000
```

oasis.reporting.database.dialect

Define a classe de dialeto do banco de dados de relatórios, definida pelo usuário.

Exemplo

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

oasis.reporting.database.ValidConnectionQuery

Define uma instrução SQL a ser executada em uma conexão antes que ela retorne do pool para verificar sua validade para testar conexões do pool obsoletas. Por exemplo: select count(*) from x.

Exemplo

```
select 1
```

oasis.reporting.database.connectionurl

Define o URL de conexão JDBC do banco de dados de relatórios.

Exemplo

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.reporting.database.additionalparamurl

Define os parâmetros adicionais a serem usados para criar a conexão do banco de dados.

Exemplo

```
;responseBuffering=full;SelectMethod=cursor;
```

FIPS_COMPLIANT

Especifica se o servidor do CA Process Automation é compatível com FIPS.

Exemplo

```
true
```

oasis.reporting.database.dbname

Define o nome do banco de dados de relatórios.

Exemplo

```
pamgacert_cluster_JDK7_rpt
```

oasis.runtime.database.dbtype

Define o tipo de banco de dados de tempo de execução.

Exemplo

```
MSSQLServer2005
```

oasis.runtime.database.username

Define o nome de usuário do servidor de banco de dados de tempo de execução.

Exemplo

```
sa
```

oasis.runtime.database.password

Define a senha associada ao usuário especificado para o servidor de banco de dados de tempo de execução.

Exemplo

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZSOIjQ79
jp66tm5E7ZYxLV2yqtVV54HRVs+xvNksG7p1pzTZOoOXahwS0XOcVoMl8Mz
nkgQgVOllCIU/YBx6lT3ZAxnzOMY2xBQnIp5xTxw0Dv5eqqTvpOnm6P2vPO
S1RzYGA6GRt3VdASiTZwZs/BkIX/sY+6C52V/x5Eg7l4hff6/6gS6wvRHdJ
G/sXU6D6
```

oasis.rntime.database.dbhostname

Define o nome do host do servidor de banco de dados de tempo de execução.

Exemplo

```
lodivsa205
```

oasis.runtime.database.port

Define o número da porta de conexão com o servidor de banco de dados de tempo de execução.

Exemplo

```
1433
```

oasis.runtime.database.dialect

Define a classe de dialeto do banco de dados de tempo de execução, definida pelo usuário.

Exemplo

```
com.optinuity.c2o.persistence.MSQLServerDialect
```

oasis.runtime.database.genericdialect

Define a classe de dialeto do banco de dados de tempo de execução.

Exemplo

```
org.hibernate.dialect.SQLServerDialect
```

oasis.runtime.database.driver

Define o nome totalmente qualificado da classe de driver do JDBC.

Exemplo

```
com.microsoft.sqlserver.jdbc.SQLServerDriver
```

oasis.runtime.database.typemapping

Define o mapeamento de tipo da fonte de dados.

Exemplo

```
MS SQLSERVER2000
```

oasis.runtime.database.exceptionsorter

Define uma classe que implementa a interface org.jboss.resource.adapter.jdbc.ExceptionSorter para examinar exceções do banco de dados para determinar se a exceção indica um erro de conexão.

Exemplo

```
org.jboss.resource.adapter.jdbc.vendor.SybaseExceptionSorte
r
```

oasis.runtime.database.ValidConnectionQuery

Define uma instrução SQL a ser executada em uma conexão antes que ela retorne do pool para verificar sua validade para testar conexões do pool obsoletas. Por exemplo: select count(*) from x.

Exemplo

```
select 1
```

oasis.runtime.database.validConnectionChecker

Define uma classe que implementa a interface org.jboss.resource.adapter.jdbc.ValidConnectionChecker para fornecer um método SQLException isValidConnection(Connection e). Uma conexão que retorna do pool chama este método para testar sua validade.

Exemplo

```
org.jboss.jca.adapters.jdbc.extensions.mssql.MSSQLValidConn
ectionChecker
```

oasis.runtime.database.datasource.class

Define a classe da fonte de dados.

Exemplo

```
com.microsoft.sqlserver.jdbc.SQLServerXADataSource
```

oasis.runtime.properties.table.create.stmt

Define a instrução SQL a ser usada para criar a tabela de propriedades, caso ela não esteja presente. Não se espera que o usuário modifique essa instrução porque, por padrão, o aplicativo configura o valor correto para o bancos de dados relevante.

Exemplo

```
create table properties (propkey varchar(255) NOT
NULL,propvalue NVARCHAR(MAX),PRIMARY KEY (propkey))
```

oasis.runtime.database.connectionurl

Define o URL de conexão JDBC do banco de dados de tempo de execução.

Exemplo

```
jdbc:sqlserver://lodivsa205:1433;databaseName=
```

oasis.runtime.database.additionalparamurl

Define os parâmetros adicionais usados para criar a conexão do banco de dados.

Exemplo

```
;responseBuffering=full;SelectMethod=cursor;
```

oasis.runtime.database.driver.name

Define o nome do driver de banco de dados de tempo de execução.

Exemplo

```
com.microsoft.sqlserver.jdbc.SQLServerDriver (para um banco
de dados MSSQL)
```

oasis.runtime.database.dbname

Define o nome do banco de dados de tempo de execução.

Exemplo

```
pamgacert_cluster_JDK7_run
```

oasis.security.server.type

Define o tipo de servidor de segurança usado para autenticação e autorização.

Exemplo

```
EEM
```

oasis.policy.type

Define o tipo de diretiva de logon.

Exemplo

```
EEM
```

certificatefolderFullpath

Define o caminho da pasta que contém o certificado de segurança. O caminho é em relação à pasta c2o.

Exemplo

```
install_dir/server/c2o/.c2orepository/public/certification/
```

oasis.eem.backend.server.location

Define o nome de host do computador que hospeda o servidor de segurança do EEM.

Exemplo

```
lodivsa205
```

oasis.eem.application.name

Define o nome do aplicativo no servidor do EEM em que as diretivas são definidas para a instância atual do CA Process Automation.

Exemplo

```
pamgacert_cluster_JDK7
```

isFipsMode

Especifica se o servidor do EEM está sendo executado no modo FIPS.

Exemplo

```
false
```

oasis.eem.certificate.path

Define o nome do certificado de segurança.

Exemplo

```
PAM.p12
```

eiamCertKeyPath

Define o nome do arquivo de chave do certificado de segurança usado para autenticação. Essa propriedade só será aplicável se isFipsMode=true.

Exemplo

```
PAM.key
```

oasis.eem.certificate.password

Define a senha associada ao certificado de segurança do EEM. Essa propriedade só será aplicável se isFipsMode=false.

Exemplo

```
aAbBcCDdeEfFgGhHiIjJkKlLmMnNoOpPqQrRsStTuUvVwWxXyYzZdD65vFT
Vmbn8aaZxjot9QCUIfPEey1H8/KGtNShgrronJk0rMtqliDMrNo2VE+xoAU
DcfmT9IPCQsAe497w1xUBkHg8PbZNjWVkPpFYw496eFiwiq7AoyB8WCoUrx
8wVnkMjoGs1BqDND+kjHcnUt9HLljYgxatT7Q2FpbTA7+Qag0W9gSv2oH4i
BsUjVs22
```

ntlm.enabled

Especifica se a autenticação NTLM está ativada. Ao alterar esta porta, remova a pasta .c2o na pasta ${Installation Dir}/server/c2o/.system, se ela existir.

oasis.jxta.port

Define a porta a ser usada para comunicação com outros orquestradores ou agentes.

Exemplo

`7001`

oasis.jxta.host

Define o nome do host do computador usado para comunicação com o orquestrador ou agente.

Exemplo

name`03-I40136.ca.com`

oasis.local.hostname

Define o nome do host do computador em que o CA Process Automation está instalado.

Exemplo

name`03-I40136.ca.com`

oasis.server.isCluster

Especifica se essa instância do CA Process Automation está agrupada.

Exemplo

`true`

loadbalancer.worker.node

Define o nome do nó no agrupamento. Esta propriedade será aplicável apenas se fizer parte do agrupamento.

Exemplo

`node2`

oasis.snmptrigger.service.port

Define a porta de escuta de disparadores do SNMP.

Exemplo

`162`

oasis.transport.secure

Especifica se a comunicação é segura.

Exemplo

`true`

AcceptAllSSLCertificates

Especifica se todos os certificados devem ser aceitos na comunicação segura.

Exemplo

`true`

oasis.reject.unnecessary.approval

Especifica se um formulário de interação que não foi configurado para aprovação deve ser rejeitado.

Exemplo

`true`

managementconsole.timeout

Define o tempo limite (em minutos) do CA Process Automation. O tempo limite é o intervalo de ociosidade permitido para o CA Process Automation, após o qual a sessão expira.

Exemplo

`30`

eem.connection.retries

Define o número de tentativas de autenticação quando o servidor de segurança for o EEM.

Exemplo

`3`

SSL_PROTOCOL

Define o tipo de protocolo SSL. Se o fornecedor de Java for a IBM Corporation, o protocolo SSL será usado. Caso contrário, será usado TLS.

Exemplo

`TLS`

X509_ALGORITHM

Define o algoritmo usado para certificados SSL. Se o fornecedor de Java for a IBM Corporation, o algoritmo usado será o IbmX509. Caso contrário, será usado SunX509.

Exemplo

`SunX509`

oasis.publisher.name

Define o nome com o qual a instância do CA Process Automation está licenciada.

Exemplo

`CA`

jboss.partition.udpgroup

Define o endereço de multitransmissão do nó de agrupamento.

Exemplo

`228.1.46.192`

jboss.rmi.port

Define a porta do serviço de nomeação de RMI.

Exemplo
`1098`

jboss.jndi.port

Define a porta de escuta do serviço bootstrap JNP(JNDI Provider).

Exemplo
`1099`

jboss.rmi.classloader.webservice.port

Define a porta usada para o serviço HTTP simples que oferece suporte a solicitações de classes para carregamento da classe dinâmica RMI, org.jboss.web.WebService.

Exemplo
`8083`

jboss.rmi.object.port

Define a porta de escuta do soquete do servidor RMI ao qual os clientes de RMI se conectam ao se comunicar por meio da interface de proxy.

Exemplo
`4444`

jboss.pooledinvoker.serverbind.port

Define a porta de vinculação de servidor do chamador em pool.

Exemplo
`4445`

remoting.transport.connector.port

Define a porta de vinculação do servidor remoto.

Exemplo
`4448`

jboss.ha.jndi.port

Define a porta na qual o stub HA-JNDI é disponibilizado.

Exemplo
`1100`

jboss.ha.jndi.rmi.port

Define a porta RMI utilizada pelo serviço HA-JNDI quando vinculado.

Exemplo
`1101`

jboss.ha.rmi.object.port

Define a porta do objeto RMI usada por JRMPInvokerHA.

Exemplo
```
4447
```

jboss.ha.pooledinvoker.serverbind.port

Define a porta de vinculação do servidor HA do chamador em pool.

Exemplo
```
4446
```

jboss.mcast.jndi.autodiscovery.port

Define a porta do grupo de multitransmissão usada para detecção automática de JNDI. Essa porta é definida em cluster-service.xml e hajndi-jms-ds.xml em deploy/jms.

Exemplo
```
1102
```

jboss.mcast.ha.partition.port

Define a porta UDP de multitransmissão para HAPartition. Essa porta é definida em cluster-service.xml e jmx-console.war/WEB-INF/web.xml.

Exemplo
```
45566
```

jboss.mcast.http.sessionreplication.port

Define a porta UDP de multitransmissão para replicação de HttpSession. Essa porta é definida em tc5-cluster-service.xml.

Exemplo
```
45567
```

tomcat.connector.http.port

Define a porta do componente conector que oferece suporte ao protocolo HTTP/1.1. Esta propriedade permite que o Catalina funcione como um servidor web autônomo, além de sua capacidade de executar servlets e páginas JSP. A porta também é configurada em jboss-ws4ee.sar/META-INF/jboss-service.xml para o Axis SService.

Exemplo
```
8080
```

tomcat.connector.ajp.port

Define a porta do componente conector que se comunica com um conector da web por meio do protocolo AJP.

Exemplo
```
8009
```

tomcat.secure.port

Define a porta segura usada pelo conector SSL. Ela não é utilizada. Essa porta é a mesma configurada como:

- redirectPort para o conector AJP em server.xml
- WebServiceSecurePort para o Axis Service em jboss-ws4ee.sar/META-INF/jboss-service.xml

A porta é usada apenas se o conector SSL estiver ativado.

Exemplo

```
8443
```

jboss.uil.serverbind.port

Define a porta à qual os clientes do serviço Unified Invocation Layer (UIL) se conectem ao estabelecer uma conexão com o servidor JBossMQ.

Exemplo

```
8093
```

oasis.protection.level

Especifica o nível de proteção do CA Process Automation. No modo de segurança, o nível de proteção é definido como CONFIDENCIAL, caso contrário ele será definido como NENHUM.

Valores: NENHUM, INTEGRAL ou CONFIDENCIAL.

itpam.initialperiodicheartbeatfrequency

Define a frequência de sinais de monitoramento inicial (em minutos).

Exemplo

```
2
```

system.encoding

Define a codificação do sistema.

Exemplo

```
Cp1252
```

eem.max.search.size

Define o número máximo de registros a serem pesquisados simultaneamente no EEM.

Exemplo

```
10000
```

jboss.remoting.transport.Connector.port

Define uma porta relacionada ao JBoss.

Exemplo

```
3873
```

OAPort

Define uma porta relacionada ao JBoss.

Exemplo

```
3528
```

OASSLPort

Define uma porta relacionada ao JBoss.

Exemplo

```
3529
```

scripts.tmpDir

Define o valor do diretório temporário que executa scripts.

Exemplo:

```
C:/Users/ADMINI~1/AppData/Local/Temp/2
```

oasis.powershell.setexecutionpolicy

Especifica se o usuário selecionou uma opção para alterar a diretiva de execução do PowerShell durante a instalação.

Exemplo

```
false
```

oasis.powershell.path

Define o caminho do PowerShell no computador host.

Exemplo

```
C:/Windows/System32/WindowsPowerShell/v1.0
```

override.jvm.tmpdir

Especifica se a variável de sistema java.io.tmpdir deve ser substituída. O valor padrão (true) permite que o servidor refira a variável de sistema para o c2oHome/tmp. Defina esta propriedade como false se não quiser que o servidor refira a variável de sistema para o c2oHome/tmp.

Exemplo

```
true
```

jboss.default.jgroups.stack

Define o tipo de pilha padrão que está sendo configurada para uso por JGroups para a execução do aplicativo.

Exemplo

```
tcp
```

jboss.jgroups.tcp.tcp_port

Define a porta TCP para agrupamento com base em TCP no JBoss.

Exemplo

```
7600
```

jboss.jgroups.tcp_sync.tcp_port

Define a porta de sincronização TCP para agrupamento com base em TCP no JBoss.

Exemplo
`7650`

jboss.messaging.datachanneltcpport

Define a porta de canal de dados de mensagens com base em TCP.

Exemplo
`7900`

jboss.messaging.controlchanneltcpport

Define a porta de canal de controle de mensagens com base em TCP.

Exemplo
`7901`

jts.default.tx.reaper.timeout

Define um número inteiro não negativo requerido pelo JBoss Transaction Service.

Exemplo
`120000`

jboss.transaction.timeout

Define o horário em que o reaper começa a fazer expirar o tempo limite das transações em andamento após esse tempo ser excedido. O JBoss requer esta propriedade.

Exemplo
`300`

jboss.service.binding.port

Define o File Ref deploy/messaging/remoting-bisocket-service.xml. O JBoss Messaging requer esta propriedade.

Exemplo
`4457`

jboss.remoting.port

Define o File Ref deploy/jmx-remoting.sar. O JBoss Remoting requer esta propriedade.

Exemplo
`1090`

jboss.jbm2.port

Define o transporte de comunicação como JBoss Messaging. O JBoss Messaging 2 Netty requer esta propriedade.

Exemplo
`5445`

jboss.hbm2,netty.ssl.port

O JBoss. A versão SSL do Netty requer esta propriedade.

Exemplo
5446

jboss.tx.recovery.manager.port

Define o File Ref deploy/transaction-jboss-beans.xml. O JBossTS Recovery Manager requer esta propriedade.

Exemplo
4712

jboss.tx.status.manager

Define o File Ref deploy/transaction-jboss-beans.xml. O JBossTS Transaction Status Manager requer esta propriedade.

Exemplo
4713

jboss.tx.manager.sock.pid.port

Define o File Ref deploy/transaction-jboss-beans.xml. O JBossTS requer esta propriedade.

Exemplo
4714

ucf.payload.file

Define o nome do arquivo que contém a carga do recipiente do Catalyst.

Exemplo
`catalyst.installer.payload.zip`

catalyst.container.name

Define o nome do recipiente do Catalyst.

Exemplo
`node0`

ucf.connector.enabled

Especifica se o Catalyst Process Automation Services está ativado.

Exemplo
`false`

ucf.payload.override

Especifica se a carga (se estiver presente) deve ser substituída.

Exemplo
`false`

ucf.pax.web.http.port

Define a porta /container/etc/org.ops4j.pax.web.cfg.

Exemplo
```
8181
```

ucf.bus.hostname

Define o nome do host do barramento do Catalyst em /registry/topology/physical/node0/catalyst-bus/bus.properties.

Exemplo
```
localhost
```

ucf.bus.port

Define a porta do barramento do Catalyst em /registry/topology/physical/node0/catalyst-bus/bus.properties.

Exemplo
```
61616
```

ucf.bus.http.port

Define a porta HTTP do barramento do Catalyst em /registry/topology/physical/node0/catalyst-bus/bus.properties.

Exemplo
```
61617
```

ucf.max.archive.query.results

Define o número máximo de resultados da consulta do arquivamento.

Exemplo
```
30
```

use.catalyst.claims.credentials

Especifica se as requisições de credenciais do Catalyst devem ser usadas.

Exemplo
```
false
```

org.apache.commons.logging.Log

Define uma classe de fábrica para instanciar agentes de log para logs comuns.

Exemplo
```
org.apache.commons.logging.impl.Log4JLogger
```

org.apache.commons.logging.LogFactory

Define uma classe de fábrica para instanciar agentes de log para logs comuns.

Exemplo
```
org.apache.commons.logging.impl.Log4jFactory
```

eem.cache.timeout

Este parâmetro adicionado pelo usuário define a duração máxima (em segundos) do cache que armazena as credenciais de usuário com o perfil de permissões associadas. Se definido como zero, este cache de autorização do CA Process Automation ficará desativado e o CA Process Automation enviará uma solicitação para o CA EEM sempre que permissões de usuário forem necessárias. Quando este parâmetro estiver ausente, o CA Process Automation usará 30 segundos como a taxa de atualização para o cache secundário.

Observação: consulte o tópico Controlar a taxa de atualização dos caches de atualizações do CA EEM (na página 78) para obter detalhes sobre os dois caches do CA EEM.

Exemplo

30

mail.attachment.buffer.size

Permite fazer download de um email com uma quantidade de buffers especificada.

K é a unidade de medida. Por exemplo, se você especificar 256, o CA Process Automation definirá como 256 K.

Exemplo

mail.attachment.buffer.size=256

mail.imap.fetchsize

Esta propriedade é específica do protocolo IMAP e não é introduzida para o CA Process Automation. Esta propriedade permite o download mais rápido de anexos de email grandes.

Especifique essa propriedade em bytes.

Exemplo

Para especificar 800 k, multiplique 800*1024.

mail.imap.fetchsize=819200